Chapter 3

Galois Theory

3.1 Preliminaries about Polynomials and Fields

Proposition 3.1.1. *Let $F \subset K$ be an extension of fields. Let $f(x), g(x) \in F[x]$. Then a g.c.d. of $f(x), g(x)$ within $F[x]$ is also a g.c.d. of $f(x), g(x)$ within $K[x]$.*

Proof. Let $d(x) \in F[x]$ be a g.c.d. for $f(x), g(x)$ within $F[x]$. Then $\exists s(x), t(x) \in F[x]$ s.t.

$$s(x)f(x) + t(x)g(x) = d(x) \tag{1}$$

Since $F[x] \subset K[x]$, this eqn. holds in $K[x]$ also.

$d(x) \mid f(x)$ and $d(x) \mid g(x)$ holds in $F[x]$ and thus holds in $K[x]$. If $h(x) \mid f(x)$ and $h(x) \mid g(x)$ within $K[x]$ then (1) $\Rightarrow h(x) \mid d(x)$ in $K[x]$. Hence $d(x)$ is a g.c.d. for $f(x), g(x)$ in $K[x]$. □

Proposition 3.1.2. *The ideal $(p(x))$ in $F[x]$ is maximal $\iff$ $p(x)$ is irreducible.*

Proof. $F[x]$ is a PID so in $F[x]$, prime $\iff$ irreducible $\iff$ maximal. □

Corollary 3.1.3. *$F[x]/(p(x))$ is a field $\iff$ $p(x)$ is irreducible.*

Theorem 3.1.4 (Eisenstein Irreducibility Criterion)**.** *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

where R is a UFD. Let $p \in R$ be prime. Suppose $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $K[x]$ where K is the field of fractions of R.

Proof. It suffices to consider the case where $\{a_0, \ldots, a_n\}$ has no common factor. Suppose $f(x)$ is reducible over K and thus (by Gauss' Lemma) reducible over R. Write

$$f(x) = (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots c_r x^s)$$

in $R[x]$, with $r < n, s < n$. Then $a_0 = b_0 c_0$. Since $p \mid a_0$ but $p^2 \nmid a_0$, p divides one of b_0, c_0 but not both. Say $p \mid b_0, p \nmid c_0$. p can't divide every b_j since then it would divide a_n, so let k be the least integer s.t. $p \nmid b_k$. So

$$a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_1 c_{k-1} + b_0 c_k.$$

$p \mid b_0, \ldots, b_{k-1}$ but $p \nmid b_k$ and $p \nmid c_0 \Rightarrow p \nmid a_k$. This is a contradiction of one of the hypotheses.
$\therefore f(x)$ is irreducible. □

3.2 Extension Fields

Suppose $F \subset K$, F, K fields. Then K is a vector space over F.

Definition 3.2.1. *The **degree** of K over F, written $[K : F]$ is the dimension of K as a v.s. $/F$. If $[K : F] < \infty$ we say K is a **finite extension** of F.*

Proposition 3.2.2. *Suppose $F \subset K \subset L$ finite extensions of fields. Then*

$$[L : F] = [L : K][K : F].$$

Proof. Let $[K : F] = n$, and let $w_1, \ldots, w_n \in K$ form a basis for K over F. Let $[L : K] = t$, and let $v_1, \ldots, v_t \in L$ form a basis for L over K. Check that $\{w_i v_j\}_{i=1,\ldots,n,\, j=1,\ldots,t}$ forms a basis for L over F:

1. Let $\ell \in L$. $v_1, \ldots, v_t$ a basis implies

   $$\ell = k_1 v_1 + k_2 v_2 + \cdots k_t v_t$$

   for some $k_1, \ldots, k_t \in K$. $w_1, \ldots, w_n$ a basis implies

   $$k_j = f_{j1} w_1 + f_{j2} w_2 + \cdots f_{jn} w_n$$

   for some $f_{j1}, \ldots, f_{jn} \in F$. Hence

   $$\begin{aligned} \ell = & f_{11}(w_1 v_1) + f_{12}(w_2 v_1) + \cdots + f_{1n}(w_n v_1) + f_{21}(w_1 v_2) + \cdots \\ & + f_{2n}(w_n v_2) + \cdots + f_{t1}(w_1 v_t) + \cdots + f_{tn}(w_n v_t). \end{aligned}$$

   $\therefore \ell$ is a linear comb. of $\{w_i v_j\}$ with coeffs. in F, so $\{w_i v_j\}$ spans L.

2. $\{w_i v_j\}_{i=1,\ldots,n,\, j=1,\ldots,t}$ is linearly independent: Suppose

   $$\begin{aligned} 0 &= f_{11} v_1 w_1 + \cdots + f_{1n} v_1 w_n + \cdots + f_{ij} v_j w_i + \cdots + f_{tn} v_t w_n \\ &= (f_{11} w_1 + f_{12} w_2 + \cdots + f_{1n} w_n) v_1 + \cdots + (f_{t1} w_1 + f_{t2} w_2 + \cdots f_{tn} w_n) v_t \end{aligned}$$

   Since $v_1, \ldots, v_t$ is a basis for L over K,

   $$f_{j1} w_1 + \cdots + f_{jn} w_n = 0 \quad \forall j = 1, \ldots, t.$$

   Since $w_1, \ldots, w_n$ is a basis for K over F, $f_{ji} = 0 \; \forall j = 1, \ldots, t, i = 1, \ldots, n$.

   $\therefore \{f_j w_i\}_{i=1,\ldots,n;\, j=1,\ldots,t}$ is linearly independent.

□

Corollary 3.2.3. *If $F \subset K \subset L$ with L a finite extension of F then* $[K : F] \mid [L : F]$.

eg. If $[L : F]$ is prime then $\nexists K$ lying strictly between F and L.
Suppose $F \subset K$ extension of fields. Let $a \in K$. Let

$$F(a) = \bigcap \{M \mid M \text{ is a field with } a \in M \text{ and } F \subset M \subset K\}.$$

Proposition 3.2.4. *$F(a)$ is a field.*

$\therefore F(a)$, the field obtained from F by adjoining a, is the smallest subfield of K containing both F and a. Explicitly,

$$F(a) = \left\{ \frac{p(a)}{q(a)} \mid p(x), q(x) \in F[x], q(a) \neq 0 \text{ in } K \right\}.$$

Proof. Let

$$M = \left\{ \frac{p(a)}{q(a)} \mid p(x), q(x) \in F[x], q(a) \neq 0 \text{ in } K \right\}.$$

Let $x = \frac{p(a)}{q(a)} \in M$. Since $F(a)$ is a field and $a \in F(a)$, field axioms $\Rightarrow p(a)$ and $q(a) \in F(a)$. $q(a) \neq 0$ $\Rightarrow \frac{1}{q(a)} \in F(a)$, so $x \in F(a)$. Hence $M \subset F(a)$.
It is easy to check that M is a field and clearly $a \in M$, so $F(a) \subset M$. □

Definition 3.2.5. *$a \in K$ is called **algebraic** over F if $\exists$ a polynomial $q(x) \in F[x]$ s.t. $q(a) = 0$ in K.*

We say that a **satisfies** the equation $q(x) = 0$ or say a is a **root** of $q(x)$ if $q(a) = 0$ in K.

Definition 3.2.6. *K is called **algebraic** over F if every element of K is algebraic over F.*

Definition 3.2.7. *If $a \in K$ is not algebraic over F then a is called **transcendental** over F.*

Note:

1. We will show that a algebraic $/F \Rightarrow [F(a) : F] < \infty$. However, K alg. $/F \not\Rightarrow [K : F] < \infty$.

   For example, let $K = \{x \in \mathbb{R} \mid x \text{ is algebraic over } \mathbb{Q}\}$. We will show later that K is a field, and by construction, K is alg. over $\mathbb{Q}$. But $[K : \mathbb{Q}] = \infty$.

2. Existence of elts. $x \in R$ s.t. x is transcendental over $\mathbb{Q}$ is easily established by a counting argument, because we will see that $\{x \in \mathbb{R} \mid x \text{ is algebraic over } \mathbb{Q}\}$ is countable. However, showing that any particular elt. of $\mathbb{R}$ is transcendental is not easy. eg. "π is transcendental" is true but nontrivial to prove.

Suppose a is algebraic over F. A polynomial $q(x) \in F[x]$ is called a **minimum polynomial** for a over F if $q(a) = 0$ and $\nexists q'(x)$ s.t. $q'(a) = 0$ with $\deg q' < \deg q$.

Given a min. polynomial for a over F, dividing by the lead coeff. gives a monic min. polynomial for a over F. A monic min. poly. of a over F is unique.

Proof. Suppose $q(x), r(x)$ are two monic min. polys. of a. By minimality, their degrees are equal. But then $s(x) = q(x) - r(x)$ has smaller degree and $s(a) = 0 - 0 = 0$. □

$\therefore$ We refer to "the min. polynomial of a".

Lemma 3.2.8. *The min. polynomial of a is irreducible.*

Proof. Let $p(x)$ be the min. poly. of a. If $p(x) = q(x)r(x)$ with $\deg q < \deg p$ and $\deg r < \deg p$ then since $p(a) = 0$, either $q(a) = 0$ or $r(a) = 0$. This is a contradiction. Hence $p(x)$ is irreducible. □

Theorem 3.2.9. *Suppose $F \subset K$, $a \in K$. Then a is algebraic over $F \iff [F(a) : F] < \infty$. More precisely, $[F(a) : F]$ = degree of the min. poly. of a.*

Proof.

$\Rightarrow$: Suppose $[F(a) : F] = n < \infty$. Consider

$$S = \{1, a, a^2, \ldots, a^n\}$$

$|S| = n + 1$. But $\dim F(a) = n$ as a v.s. $/F$. So the elts. of S are linearly dependent.
ie. $\exists$ relation

$$c_0 + c_1 a + c_2 a^2 + \cdots c_n a^n = 0$$

where $c_j \in F$ and not all c_j are 0. Hence a satisfies $q(x) = 0$ where

$$q(x) = c_0 + c_1 x + c_2 x^2 + \cdots c_n x^n.$$

$\therefore$ a is algebraic over F.

$\Leftarrow$: Suppose a is alg. over F. Let

$$p(x) = p_0 + p_1 x + \cdots + x^n$$

be the min. poly. of a over F.

Claim. $B = \{1, a, a^2, \ldots, a^{n-1}\}$ forms a basis for $F(a)$ over F.

Proof. If B were linearly dependent then (as above) there would be a polynomial of degree $n-1$ or less satisfied by a, contradicting defn. of $p(x)$.

Show B spans $F(a)$: $p(a) = 0$ so

$$a^n = -p_0 - p_1 a - \cdots - p_{n-1}a^{n-1}$$

and thus, $a_n \in \text{span}B$.

$$\begin{aligned} a^{n+1} &= a \cdot a^n \\ &= -p_0 a - p_1 a^2 - \cdots - p_{n-2}a^{n-1} - p_{n-1}a^n \\ &= -p_0 a - p_1 a^2 - \cdots - p_{n-2}a^{n-1} - p_{n-1}(-p_0 - p_1 a - \cdots - p_{n-1}a^{n-1}) \end{aligned}$$

$\in \text{span}B$

etc. ie. By induction, $a^s \in \text{span}B \; \forall s$, so $F[a] \subset \text{span}B$.

So to finish the proof, it suffices to show:

Lemma 3.2.10. $F(a) = F[a]$.

Proof. $F[a] \subset F(a)$ is trivial. Conversely, let $x \in F(a)$, $x = \frac{q(a)}{r(a)}$ where $q(a), r(a) \in F[a]$ and $r(a) \neq 0$. $p(x) \nmid r(x)$ since $r(a) \neq 0$. Since $p(x)$ is irreducible, this implies $p(x), r(x)$ have no common factors, ie. $\gcd(p(x), r(x)) = 1$. So, $\exists$ polynomials $s(x), t(x)$ s.t.

$$s(x)p(x) + t(x)r(x) = 1.$$

$\therefore 1 = s(a)p(a) + t(a)r(a) = t(a)r(a)$. Thus, $\frac{1}{r(a)} = t(a)$ and

$$x = \frac{q(a)}{r(a)} = q(a)t(a) \in F[a].$$

$\therefore F(a) \subset F[a]$. □

Corollary 3.2.11. *Suppose $F \subset K$. Suppose $a \in K$ is algebraic over F and let $q(a) \in F[x]$ be the min. poly. of a over F. Then*

$$F(a) \cong F[x]/(q(x)).$$

Proof. Let $\phi : F[x] \mapsto F(a)$ be given by

$$\phi(p(x)) = p(a).$$

Since $F(a) = F[a]$, ϕ is onto.
Claim. $\ker \phi = (q(x))$.

Proof. Let $\ker \phi = (q'(x))$ where q' is monic. Then since $q(a) = 0$, $q'(x) \mid q(x)$. But $q(x)$ is irreducible, so either $q'(x) = 1$ or $q'(x) = q(x)$. Since $q'(a) = 0$, $q'(x) \neq 1$ so $q'(x) = q(x)$.

Thus, by 1st isomorphism theorem,

$$F(a) = \Im\phi \cong F[x]/\ker\phi = F[x]/(q(x).$$

□

Theorem 3.2.12. *Suppose $F \subset K$ are fields. Let*

$$M = \{x \in K \mid x \text{ is algebraic over } F\}.$$

Then M is a field.

Proof. Let $a, b \in M$. Must show $a \pm b, ab, a/b \in M$. Suppose $[F(a) : F] = m$ and $[F(b) : F] = n$. So b satisfies a degree n poly. $p(x)$ with coeffs in $F \subset F(a)$. $p(x)$ can be thought of as a polynomial in $F(a)[x]$, giving

$$[F(a)(b) : F(a)] \leq n.$$

Hence

$$[F(a)(b) : F] \leq nm.$$

Since $a + b \in F(a)(b)$,

$$F \subset F(a + b) \subset F(a)(b).$$

$\therefore [F(a + b) : F] \leq nm$, and so $a + b$ is algebraic over F. Similarly, $a - b, ab, a/b \in F(a)(b)$ so the same argument applies. □

Notation: $F(a, b) = F(a)(b)$. Observe that $F(a, b) = F(b, a)$ is the smallest subfield of K containing F, a, b.

Corollary 3.2.13. *Suppose $F \subset K \subset L$. If K is algebraic over F and L is algebraic over K then L is algebraic over F.*

Proof. Let $z \in L$. L algebraic over $K \Rightarrow z$ satisfies $p(z) = 0$ where

$$p(x) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$$

has coeffs. in K. So $F \subset F(c_1, \ldots, c_n) \subset K \subset L$. Since K is algebraic over F, each c_j is algebraic over F.

If m_j is the degree of the min. poly. of c_j over F then, as above,

$$[F(c_1, \ldots, c_n) : F] \leq m_1 \cdots m_n < \infty.$$

Since z satisfies the polynomial $p(x)$ whose coeffs. lie in $F(c_1, \ldots, c_n)$,

$$[F(c_1, \ldots, c_n, z) : F(c_1, \ldots, c_n)] < \infty.$$

$\therefore [F(c_1, \ldots, c_n, z) : F] < \infty$. But $F \subset F(z) \subset F(c_1, \ldots, c_n, z)$ so $[F(z) : F] < \infty$. Thus, z is algebraic over F.

This is true for all $z \in L$, so L is algebraic over F. □

Example 3.2.14. *Let*

$$M = \{x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q}\}.$$

Our theorems show that M is a field, and by construction, it is algebraic over $\mathbb{Q}$. However, in $\mathbb{Q}[x]$, there are irreducible polynomials of arbitrarily large degree, and by definition, the roots of these polynomials are in M. So $[M : \mathbb{Q}]$ is unbounded.

3.3 Roots

Let F be a field and let $p(x) \in F[x]$. p might have no roots in F.

Question. Given $p(x) \in F[x]$, can we always find an extension field $K \supset F$ in which $p(x)$ has a root?

Theorem 3.3.1 (Remainder Theorem)**.** *Let K be a field. Let $p(x) \in K[x]$ and let $b \in K$. Then $\exists q(x)$ s.t. $p(x) = (x-b)q(x) + p(b)$, and* $\deg q(x) = (\deg p(x)) - 1$.

Proof. By division algorithm, $p(x) = (x-b)q(x)+r(x)$ where $\deg r < \deg(x-b) = 1$. ie. $r(x) = r \in K$.
Setting $x = b$,

$$p(b) = (b-b)q(b) + r = r.$$

Comparing degrees of LHS and RHS, $\deg q(x) = (\deg p(x)) - 1$. □

Corollary 3.3.2 (Factor Theorem)**.** *a is a root of $p(x) \iff (x-a) \mid p(x)$.*

Proof. $p(x) = (x-a)q(x) + p(a)$. If $p(a) = 0$ then $p(x) = (x-a)q(x)$ so $(x-a) \mid p(x)$. Conversely, if $p(x)$ is a multiple of $x-a$ then $p(a) = 0$. □

Definition 3.3.3. *The **multiplicity** of a root a of $p(x)$ is the largest power of $(x-a)$ which divides $p(x)$.*

Corollary 3.3.4. *A polynomial of degree n over a field K can have at most n roots (counted with multiplicity).*

Proof. A polynomial of degree 1 has exactly one root, so the result follows from the Factor Thm. by induction. □

Theorem 3.3.5. *Let $p(x) \in F[x]$ be a poly of degree n where F is a field. Then $\exists$ an extension field K of F with $[K : F] \leq n$ in which $p(x)$ has a root.*

Proof. Let $q(x)$ be an irred. factor of $p(x)$. Since any root of $q(x)$ is a root of $p(x)$ we will find an extension field in which $q(x)$ has a root. Let

$$K = F[x]/(q(x)).$$

$q(x)$ irreducible $\Rightarrow K$ is a field. $F \hookrightarrow K$ by $c \mapsto [c]$, so K is an extension field of F.

In K, $q([x]) = [q(x)] = 0$. So $a = [x]$ is a root of $q(x)$. Since $q(x)$ is irreducible over F, $q(x)$ is the min. poly. of a over F.
$\therefore K = F(a)$ and

$$\begin{aligned}[K : F] &= [F(a) : F] \\ &= \deg(\text{min. poly of } a) \\ &= \deg q \\ &\leq \deg p = n.\end{aligned}$$

□

Example 3.3.6. *Let $F = \mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$. $(x^2 + x + 1)$ is irred. in $\mathbb{F}_2[x]$. Let*

$$K = \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}.$$

Let $w = [x] \in K$, so $w^2 + w + 1 = [x^2 + x + 1] = 0$.

In K we have four elements: $0, 1, w, w + 1$. Multiplication is as follows: Mult. by 0 and 1 is obvious.

$$w^2 = -w - 1 = w + 1$$
$$w(w - 1) = w^2 + 1 = w + 1 + w = 1$$
$$(w - 1)^2 = w^2 + 2w + 1 = w + 1 + 1 = w$$

Note $\frac{1}{w} = w - 1$ and $\frac{1}{w-1} = w$ (every nonzero elt. has an inverse).

$$K = \mathbb{F}_4$$

(finite field with 4 elements).

By induction on the previous result, we get

Corollary 3.3.7. *Let $p(x) \in F[x]$ be a poly. of degree n (F a field). Then $\exists$ an extension field K of F with $[K : F] \leq n!$ in which $p(x)$ has n roots. ie. In K we can factor $p(x)$ completely as*

$$p(x) = \lambda(x - a_1)(x - a_2) \cdots (x - a_n).$$

Example 3.3.8.

1. *$F = \mathbb{Q}$, $p(x) = x^3 - 2$. Let $E_1 = F(2^{\frac{1}{3}})$ Then $[E_1 : F] = 3$. In E_1,*

$$p(x) = (x - 2^{\frac{1}{3}})(x^2 + 2^{\frac{1}{3}}x + 2^{\frac{2}{3}}).$$

Let $K = E_1(\sqrt{3}i)$. Then $[K : E_1] = 2$ so $[K : F] = 3 \cdot 2 = 6$. In K,

$$p(x) = (x - 2^{\frac{1}{3}})\left(x + \frac{2^{\frac{1}{3}}(1 - \sqrt{3}i)}{2}\right)\left(x + \frac{2^{\frac{1}{3}}(1 + \sqrt{3}i)}{2}\right).$$

2. *$F = \mathbb{Q}$, $p(x) = x^3 - 12x + 8$. Let $M = -4 + 4\sqrt{3}i$. Let $z = M^{\frac{1}{3}}$ (that is, z is any one of the three elts. s.t. $z^3 = -4 + 4\sqrt{3}i$). Let $a = z + \overline{z}$.*

So $\overline{z}^3 = \overline{M}$ and

$$z\overline{z} = (M\overline{M})^{\frac{1}{3}} = (16 + 48)^{\frac{1}{3}} = 64^{\frac{1}{3}} = 4.$$

Thus

$$\begin{aligned} a^3 &= (z+\overline{z})^3 \\ &= M + \overline{M} + 3z^2\overline{z} + 3z\overline{z}^2 \\ &= M + \overline{M} + 3(z\overline{z})(z+\overline{z}) \\ &= M + \overline{M} + 3z\overline{z}a \\ &= -8 + 3\cdot 4\cdot a \\ &= -8 + 12a \end{aligned}$$

$\therefore a^3 - 12a + 8 = 0$. *Let* $E_1 = \mathbb{Q}(a)$, *so* $[E : F] = 3$. *Let* $b = \frac{a^2-8}{2} \in E_1$. *Then*

$$\begin{aligned} b^3 &= \frac{a^6 - 12a^4 + 3\cdot 64a^2 - 8^3}{8} \\ &= \frac{(12a-8)^2 - 24a(12a-8) + 3\cdot 64a^2 - 8^3}{8} \\ &= \frac{16(9a^2 - 12a + 4) - 24(12a^2 - 8a) + 3\cdot 64a^2 - 8^3}{8} \\ &= 18a^2 - 24a + 8 - 36a^2 + 24a + 24a^2 - 64 = 6a^2 - 56 \end{aligned}$$

$$\begin{aligned} 12b - 8 &= 12\left(\frac{a^2-8}{2}\right) - 8 \\ &= 6(a^2 - 8) - 8 \\ &= 6a^2 - 48 - 8 \\ &= 6a^2 - 56 \end{aligned}$$

$\therefore b^3 - 12b + 8 = 0$. *Note that this second root is already in* E_1. *Let* c *be the third root. Then*

$$a + b + c = \textit{coeff. of } x^2 \textit{ in } p(x) = 0.$$

$\therefore c = -a - b \in E_1$. *So all* 3 *roots lie in* E_1. *In* E_1, $x^3 - 12x + 8$ *factors as* $(x-a)(x-b)(x-c)$.

Definition 3.3.9. *Let* $p(x) \in F[x]$. *An extension field* K *of* F *is called a* ***splitting field*** *for* $p(x)$ *over* F *if* $p(x)$ *factors completely in* K *into linear factors*

$$p(x) = \lambda(x - a_1)(x - a_2)\cdots(x - a_n)$$

and $p(x)$ *does not factor completely in any proper subfield of* K.

ie. K is a minimal extension of F containing all roots of $p(x)$. By an earlier theorem, a poly. of degree n in $F[x]$ has a splitting field K s.t. $[K : F] \leq n!$.

Proposition 3.3.10. *Suppose $F \subset M \subset K$. Let $p(x) \in F[x]$ and suppose that K is a splitting field of $f(x)$ over F. Then regarding $p(x)$ as an elt. of $M[x]$, K is also a splitting field of $p(x)$ over M.*

Proof. Trivial. □

Example 3.3.11.

1. *$p(x) = x^3 - 2$, $F = \mathbb{Q}$. $2^{\frac{1}{3}}$ is a root of $p(x)$ but $\mathbb{Q}(2^{\frac{1}{3}})$ is not a splitting field for $p(x)$. $K = \mathbb{Q}(2^{\frac{1}{3}}, \sqrt{3}i)$ is a splitting field for $p(x)$, and $[K : \mathbb{Q}] = 6$.*
2. *$p(x) = x^3 - 12x + 8$, $F = \mathbb{Q}$. $a = z + \bar{z}$ where $z^3 = -4 + 4\sqrt{3}i$. a is a root of $p(x)$ and $K = \mathbb{Q}(a)$ is a splitting field for $p(x)$. In this case, $[K : \mathbb{Q}] = 3$.*

Proposition 3.3.12. *Let $K \supset F$ be a splitting field for $p(x) \in F[x]$. Suppose that in K,*

$$p(x) = \lambda(x - a_1)(x - a_2) \cdots (x - a_n),$$

where $\lambda \in K$. Then

$$K = F(a_1, \ldots, a_n).$$

Proof. By defn of $a_1, \ldots, a_n$ they lie in K so $F(a_1, \ldots, a_n) \subset K$. However, if all of $a_1, \ldots, a_n$ lay in some proper subfield of K then the factorization

$$p(x) = \lambda(x - a_1)(x - a_2) \cdots (x - a_n)$$

would be valid in that subfield, contradicting the minimality of K. □

Recall that if $a \in K$ is a root of an irreducible poly. $p(x) \in F[x]$ then

$$F(a) \cong F[x]/(p(x))$$

where the isomorphism $\psi : F[x]/(p(x)) \overset{\cong}{\longmapsto} F(a)$ is given by $\psi(x) = a$. Suppose $\tau : F \overset{\cong}{\longmapsto} F'$. τ extends to

$$\begin{aligned} \tilde{\tau} : F[x] &\overset{\cong}{\longmapsto} F'[x] \\ x &\longmapsto x \\ f &\longmapsto \tau(f) \quad \forall f \in F. \end{aligned}$$

Theorem 3.3.13. *Let $p(x) \in F[x]$ be irreducible. Let $p' = \tilde{\tau}(p) \in F'[x]$. Let a, a' be roots of $p(x), p'(x)$ lying in extension fields of F, F' respectively. Then τ can be extended to an isomorphism*

$$\phi : F(a) \overset{\cong}{\longmapsto} F(a')$$

s.t. $\phi(a) = a'$.

Proof. We have

$$F(a) \overset{\cong}{\longleftarrow} \psi\frac{F[x]}{(p(x))} \overset{\cong}{\longrightarrow} \tilde{\tau}\frac{F'[x]}{(p'(x))} \overset{\cong}{\longrightarrow} \psi' F'(a')$$

Let $\phi = \psi' \circ \tilde{\tau} \circ \psi^{-1}$. □

Example 3.3.14. *$F = F' = \mathbb{Q}$, $\tau = 1_{\mathbb{Q}}$, $p(x) = p'(x) = x^3 - 2$. $a = 2^{\frac{1}{3}}, a' = 2^{\frac{1}{3}}\left(\frac{1-\sqrt{3}i}{2}\right)$. Using $a^3 = 2$, elts. of $\mathbb{Q}(a)$ can be expressed in the form $\alpha + \beta a + \gamma a^2$, $\alpha, \beta, \gamma \in \mathbb{Q}$. $\phi : \mathbb{Q}(a) \overset{\cong}{\longmapsto} \mathbb{Q}(a')$ is given by*

$$\phi(\alpha + \beta a + \gamma a^2) = \alpha + \beta a' + \gamma (a')^2.$$

Theorem 3.3.15. *Let $p(x) \in F[x]$. Let $p' = \tilde{\tau}(p) \in F'[x]$. Let E, E' be splitting fields of $p(x), p'(x)$ respectively. Then τ can be extended to an isomorphism $\phi : E \overset{\cong}{\longmapsto} E'$.*

In particular, letting $F' = F$ and $\tau = 1_F$ shows that any two splitting fields of $p(x)$ are isomorphic, by an isomorphism which fixes F.

Proof. Use induction on $[E : F]$. If $[E : F] = 1$ then $E = F$ so $p(x)$ splits into linear factors in F. But then $p'(x)$ splits into linear factors in F' so $E' = F'$, and use $\phi = \tau$.

Now let $[E : F] = n > 1$. Assume by induction that the theorem holds whenever $[E : F] < n$. More precisely, assume that the following statement holds: let $q(x) \in M[x]$ be a poly. over a field M, $\sigma : M \overset{\cong}{\longmapsto} M'$, $q' = \tilde{\sigma}(q)$. Let N, N' be splitting fields of q, q' respectively. If $[N : M] < n$ then σ can be extended to an iso. $\phi : N \overset{\cong}{\longmapsto} N'$.

Let $s(x)$ be a non-linear irreducible factor of $p(x)$ in $F[x]$. Let $\deg s(x) = r > 1$. Let $v \in E$ be a root of $s(x)$. Let $w \in E'$ be a root of $\tilde{\tau}(s)$. By prev. thm. $\exists$ iso. $\sigma : F(v) \overset{\cong}{\longmapsto} F'(w)$ s.t. $\sigma|_F = \tau$ and $\sigma(v) = w$. Since $\deg s(x) = r$, $[F(v) : F] = r$, so

$$[E : F(v)] = \frac{[E : F]}{[F(v) : F]} = \frac{n}{r} < n.$$

From an earlier proposition, E is a splitting field for $p(x)$ considered as a poly. in $F(v)[x]$, and likewise, E' is a splitting field for $p'(x)$ considered as a poly. in $F'(w)[x]$. So by the induction hypothesis, $\exists$ iso. $\phi : E \overset{\cong}{\longmapsto} E'$ s.t. $\phi|_{F(v)} = \sigma$. Thus $\phi|_F = \sigma|_F = \tau$ as required. □

3.4 Characteristic

Theorem 3.4.1. *Let R be an integral domain. Let H be the additive subgroup of R generated by* 1. *Then either $H \cong \mathbb{Z}$ or $H \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Proof. Define $\phi : \mathbb{Z} \mapsto F$ to be the group homomorphism determined by $\phi(1) = 1$. Then

$$H = \mathrm{Im}\phi \cong \mathbb{Z}/\ker\phi.$$

$\ker\phi$ is an ideal in $\mathbb{Z}$ so $\ker\phi = (n)$ for some n. If $n = 0$ then $H \cong \mathbb{Z}$. Otherwise, $H \cong \mathbb{Z}/n\mathbb{Z}$ (as groups), and by replacining n by $-n$ if necessary, we may assume $n > 0$.

If $a, b \in \mathbb{Z}, a, b > 0$ then in R,

$$\phi(a)\phi(b) = \overbrace{(1 + \cdots + 1)}^{a \text{ times}}\overbrace{(1 + \cdots + 1)}^{b \text{ times}} = \overbrace{(1 + \cdots + 1)}^{ab \text{ times}} = \phi(ab).$$

So $H \cong \mathbb{Z}/nZ$ as rings, and R is an integral domain, so p must be prime. □

Definition 3.4.2. *If the additive subgroup of an integral domain R generated by* 1 *is $\mathbb{Z}/p\mathbb{Z}$, we say that R has **characteristic** p, and denote* $\mathrm{char}\, R = p$. *If this subgroup is $\mathbb{Z}$, we say* $\mathrm{char}\, R = 0$.

If F is a field with $\mathrm{char}\, F = p$, we can define

$$\begin{aligned} \theta : \mathbb{Z}/p\mathbb{Z} &\mapsto F \\ 1 &\mapsto 1 \end{aligned}$$

as an inclusion of fields. If $\mathrm{char}\, F = 0$, we can define

$$\begin{aligned} \theta : \mathbb{Q} &\mapsto F \\ 1 &\mapsto 1 \\ \frac{s}{t} &\mapsto \overbrace{(1 + \cdots + 1)}^{s \text{ times}} / \overbrace{(1 + \cdots + 1)}^{t \text{ times}} \end{aligned}$$

The image of θ is a subfield of F (isomorphic to either $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ or $\mathbb{Q}$), called the **prime field** of F.

Proposition 3.4.3. *If* $\mathrm{char}\, F = p$ *then in F,*

$$(a + b)^{p^k} = a^{p^k} + b^{p^k}.$$

Proof.

$$(a+b)^{p^k} = \sum_{i=0}^{p^k} \binom{p^k}{i} a^i b^{p^k-i} = a^{p^k} + b^{p^k} + \sum_{i=1}^{p^k-1} \binom{p^k}{i} a^i b^{p^k-i}.$$

If $1 \le i \le p^k - 1$ then

$$\begin{aligned}\binom{p^k}{i} &= \frac{p^k!}{i!(p^k-i)!} \\ &= \frac{p^k(p^k-1)\cdots(p^k-i+1)}{1\cdot 2\cdot 3\cdots i} \\ &= \left(\frac{p^k}{i}\right)\left(\frac{p^k-1}{1}\right)\left(\frac{p^k-2}{2}\right)\cdots\left(\frac{p^k-i+1}{i-1}\right).\end{aligned}$$

For $1 \le j < p^k$, the number of factors of p in j = the number of factors of p in $p^k - j$. However, since $i < p^k$, p^k has more factors of p than i does. Hence, the numerator has more factors of p than the denominator. ie. $p \left| \binom{p^k}{i} \right.$ for $0 < i < p^k$. Since $\operatorname{char} F = p$,

$$\sum_{i=1}^{p^k-1} \binom{p^k}{i} a^i b^{p^k-i} = 0.$$

□

3.5 Repeated Roots

Notation: For $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, set

$$f'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-1} + \cdots + a_1.$$

$f'(x)$ is called the **derivative** of $f(x)$.
Note: If $\operatorname{char} F = p \neq 0$ then $f'(x) = 0 \Rightarrow f(x)$ is constant. For example, $f(x) = x^p$ has $f'(x) = 0$.

Theorem 3.5.1. *$f(x)$ has a repeated root (in some extension field of F) $\iff$ $f(x), f'(x)$ have a common factor.*

Proof. Let K be the splitting field of f.

Note that $f(x), f'(x)$ have a common factor $\iff \gcd(f, f') \neq 1$. Moreover, as seen before, the g.c.d. is the same whether taken in $F[x]$ or $K[x]$.

$\Rightarrow$: Suppose $f(x)$ has a repeated root. In $K[x]$, $f(x) = (x-\alpha)^2 q(x)$, so

$$f'(x) = 2(x-\alpha)q(x) + (x-\alpha)^2 q'(x) = (x-\alpha)(2q(x) + (x-\alpha)q'(x)).$$

$\therefore \gcd(f, f') \neq 1$ in K and thus in F.

$\Leftarrow$: Suppose $f(x), f'(x)$ have a common factor. If $f(x)$ has no repeated root then by (WLOG) taking $f(x)$ to be monic, in $K[x]$,

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

where $\alpha_j \neq \alpha_k$ for $j \neq k$. So

$$f'(x) = \sum_{i=1}^{n} (x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_r).$$

If $(x-\alpha_j)$ is also a factor of $f'(x)$ then α_j would be a root of $f'(x)$ giving

$$0 = \prod_{j \neq i} (\alpha_j - \alpha_i).$$

But then $\alpha_j - \alpha_i = 0$ for some i, which is a contradiction. Thus, $f(x)$ has a repeated root.

□

Corollary 3.5.2. *Let $f(x) \in F[x]$ be irreducible. Then*

1. *If* $\operatorname{char} F = 0$ *then* $f(x)$ *has no repeated roots.*

2. *If* $\operatorname{char} F = p > 0$ *then* $f(x)$ *has a repeated root* $\iff f(x) = g(x^p)$ *for some* g.

Proof. If $f(x)$ has a repeated root then $f(x)$, $f'(x)$ have a common factor. But $f(x)$ is irreducible and $\deg f'(x) < \deg f(x)$. Thus $f'(x) = 0$.

If $\operatorname{char} F = 0$ then $f'(x) = 0 \Rightarrow f(x)$ is constant, in which case, $f(x)$ does not have a repeated root after all.

If $\operatorname{char} F = p$, let

$$f(x) = a_0 + a_1 x + \cdots + a_p x^p + a_{p+1} x^{p+1} + \cdots + a_n x^n.$$

Since $f'(x) = 0$, $a_k = 0$ for every k which is not a multiple of p. So

$$f(x) = a_p x^p + a_{2p} x^{2p} + \cdots = g(x^p).$$

□

3.6 Finite Fields

Proposition 3.6.1. *Let F be a field with q elements. Suppose $F \subset K$ is a finite extension with $[K : F] = n$. Then K has q^n elements.*

Proof. As a vector space, $K \cong F^n$, so $|K| = |F|^n = q^n$. □

Corollary 3.6.2. *Let K be a finite field. Then K has p^m elements for some m where $p = \operatorname{char} F$.*

Proof. Let F be the prime field of K. Since K is finite, F cannot be $\mathbb{Q}$, so $\operatorname{char} F = p$, a prime. Hence K has p^m elements where $m = [K : F]$. □

Corollary 3.6.3 (Fermat)**.** *Let F be a finite field with p^m elements. Then $a^{p^m} = a$ for all $a \in F$.*

Proof. If $a = 0$ then $a^{p^m} = 0$. If $a \neq 0$ then $a \in F - \{0\}$, which forms a group under multiplication, and

$$|F - \{0\}| = p^m - 1.$$

By Lagrange, $a^{p^m-1} = 1$, so $a^{p^m} = a$. □

Theorem 3.6.4. *Let F be a finite field with p^n elements. Then in $F[x]$, $x^{p^n} - x$ factors as*

$$x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha).$$

Proof. By the previous corollary, every elt. of F is a root of $x^{p^n} - x$. Since $\deg(x^{p^n} - x) = p^n$, and F has p^n elements, we have all the roots. □

Corollary 3.6.5. *If F has p^n elements then F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.*

Corollary 3.6.6. *Any two finite fields with the same number of elts. are isomorphic.*

Proof. Any two splitting fields of the same polynomial are isomorphic. □

Theorem 3.6.7. *For every prime p and every positive integer n, $\exists!$ a field with p^n elts.*

Proof. We have already shown that $\exists$ at most one field with p^n elts. So, show that one exists.

Let K be the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. Let

$$F = \{a \in K \mid a^{p^n} = a\}.$$

$f'(x) = -1$, which is relatively prime to $f(x)$. So the roots of $f(x)$ are distinct, ie. F has p^n elts., and it suffices to show that F is a field.

Suppose $a, b \in F$. Then

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$$

so $a + b \in F$. Similarly, $(a-b)^{p^n} = a - b$.

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab$$

and similarly, $(\frac{a}{b})^{p^n} = \frac{a}{b}$. Hence F is a field. □

Theorem 3.6.8. *Let G be a finite abelian group s.t. $\forall n \in \mathbb{Z}$, there are at most n elts. of G satisfying $g^n = e$. Then G is a cyclic group.*

Proof. By the structure theorem for finitely generated abelian groups, we can write

$$G \cong G_1 \times G_2 \times \cdots \times G_k$$

where $|G_j| = p_j^{t_j}$ for some p_j with $p_j \neq p_{j'}$ if $j \neq j'$. Since $C_n \times C_m \cong C_{nm}$ when $\gcd(n, m) = 1$, it suffices to show that each G_j is a cyclic group.

Pick j and write p for p_j and t for t_j. Let $a \in G_j$ be an elt. whose order is maximal. Then

$$|a| \,\Big|\, |G_j| = p^t$$

so $|a| = p^r$ for some $r \leq t$. Within G_j,

$$S = \{a, a^2, \cdots, a^{p^r - 1}, e\}$$

are the distinct roots of $g^{p^r} = e$, by construction of a. Since there are p^r of them, by the hypothesis, g^{p^r} has no other solutions in G, and in particular, no other solutions in G_j.

Now let $b \in G_j$. Then $|b| = p^s$ for some $s \leq r$.

$$b^{p^r} = \left(b^{p^s}\right)^{p^{r-s}} = e^{p^{r-s}} = e.$$

Thus, $b \in S$, ie. $b = a^i$ for some i.

Hence G_j is cyclic, so G is cyclic. □

Corollary 3.6.9. *Let F be a field. Then any finite subgroup of the multiplicative group of $F - \{0\}$ is cyclic.*

Proof. Since F is a field, a polynomial of degree n in $F[x]$ has at most n roots in F. □

Corollary 3.6.10. *If F is a finite field then the multiplicative group $F - \{0\}$ is cyclic.*

3.7 Separable Extensions

Definition 3.7.1. *Suppose $F \subset K$ is a finite extension. Then $\alpha \in K$ is called **separable** over F if its irreducible polynomial over F has no repeated roots. K is called separable over F if α is separable over F $\forall \alpha \in K$.*

Proposition 3.7.2. *If* $\operatorname{char} F = 0$ *then every finite extension of F is separable over F.*

Example 3.7.3. *Let E be any field with* $\operatorname{char} E = p$. *Let $F = E(z)$, the field of fractions of $E[z]$. Let $K = F(z^{\frac{1}{p}})$, and let $a = z^{\frac{1}{p}} \in K$. Then the min. poly. of a over F is $x^p - z = (x-a)^p$. Hence, $z^{\frac{1}{p}}$ is not separable over F.*

Theorem 3.7.4. *Suppose $F \subset K$ is separable. Then $\exists \gamma \in K$ s.t. $K = F(\gamma)$.*

Proof.

Case 1: F is finite.

Since $F \subset K$ is a finite extension, K is also a finite field. Let c be a generator for the cyclic group $K - \{0\}$.

$$\text{ie.} \quad K - \{0\} = \{c, c^2, \cdots, c^{p^m-1}, e\}.$$

$\therefore$ Any field containing c contains all of $K - \{0\}$. $\therefore K = F(c)$.

Case 2: $|F| = \infty$.

Since $[K : F] < \infty$, let $K = F(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n$. Using induction, it suffices to consider the case $n = 2$. ie. Suppose $K = F(a, b)$ and show that $\exists c$ s.t. $F(a, b) = F(c)$.

Let $f(x), g(x)$ be the min. polynomials of a, b respectively. Let M be the splitting field of $f(x)g(x)$. In M,

$$f(x) = (x - a_1) \cdots (x - a_m) \quad \text{where } a_1 = a$$
$$g(x) = (x - b_1) \cdots (x - b_n) \quad \text{where } b_1 = b.$$

Since K is separable, $a_i \neq a_j$ for $i \neq j$ and $b_i \neq b_j$ for $i \neq j$. Consider the equation

$$a_i + \lambda b_j = a_1 + \lambda b_1$$

where $j > 1$ and $\lambda \in F$. The solution for λ is

$$\lambda = \frac{a_i - a_1}{b_1 - b_j}$$

Since F is finite, choose $\gamma \in F$ s.t. $\gamma \neq \frac{a_i - a_1}{b_1 - b_j}$ and $\gamma \neq \frac{b_j - b_1}{a_1 - a_j}$ for any i and j. So $a_i + \gamma b_j \neq a + \gamma b$ unless $i = j = 1$. Set $c := a + \gamma b$.

Claim. $F(a, b) = F(c)$.

Proof. $c \in F(a,b)$ so $F(c) \subset F(a,b)$. So show $F(a,b) \subset F(c)$, ie. show $a \in F(c)$ and $b \in F(c)$.

Let $h(x) = f(c - \gamma x) \in F(c)[x]$. Then

$$h(b) = f(c - \gamma b) = f(a) = 0.$$

By construction, $c - \gamma b_j \neq a_i$ unless $i = j = 1$. So if $j > 1$ then $c - \gamma b_j \neq a_i$ for any i and so $c - \gamma b_j$ is not a root of $f(x)$.

$\therefore$ If $j > 1$ then $h(b_j) = f(c - \gamma b_j) \neq 0$. Hence $b = b_1$ is the only common root of $g(x)$ and $h(x)$. ie. In $K[x]$,

$$\gcd(g(x), h(x)) = x - b.$$

But $g(x) \in F[x] \subset F(c)[x]$ and $h(x) \in F(c)[x]$, so by an earlier proposition,

$$x - b = \gcd(g(x), h(x)) \in F(c)[x].$$

In particular, $x - b \in F(c)[x]$; that is, its coefficients lie in $F(c)$. So $b \in F(c)$.

Similarly, using $\gamma \neq \frac{b_j - b_1}{a_1 - a_i}$ for any i and j gives $a \in F(c)$. Thus $F(a,b) \subset F(c)$ as required.

□

3.8 Automorphism Groups

Definition 3.8.1. *An isomorphism from a field to itself is called an* ***automorphism****. Explicitly, an automorphism* $\sigma : F \xrightarrow{\cong} F$ *must satisfy:*

1. σ *is a bijection,*
2. $\sigma(a+b) = \sigma(a) + \sigma(b)$*, and*
3. $\sigma(ab) = \sigma(a)\sigma(b)$*.*

Let $\mathrm{Aut}(F)$ *denote the set of all automorphisms of* F*. This forms a group under composition.*

Theorem 3.8.2. *Let* $\sigma_1, \ldots, \sigma_n$ *be distinct automorphisms of* F*. Then* $\sigma_1, \ldots, \sigma_n$ *are linearly independent in the vector space* $\hom_{\textit{abel. grps.}}(F, F)$*.*

ie. If $a_1, \ldots, a_n \in F$ such that

$$a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0 \quad \forall u \in F$$

then $a_1 = a_2 = \cdots = a_n = 0$.
Note: This proof works equally well to show that distinct homomorphisms from a ring A to a field F are linearly independent in the F-vector space $\hom_{\text{abel. grps.}}(A, F)$.

Proof. Suppose $\sigma_1, \ldots, \sigma_n$ are not linearly independent in $\hom_{\text{abel. grps.}}(F, F)$. Find a relation having as few terms as possible. Renumber the σ's so that the terms appearing in the relation come first. So the relation is

$$a_1\sigma_1 + \cdots + a_k\sigma_k = 0$$

with $a_j \neq 0$ for $j = 1, \ldots, k$, and no relation exists involving fewer than k terms. That is, for all $u \in F$,

$$a_1\sigma_1(u) + \cdots + a_k\sigma_k(u) = 0 \tag{1}$$

If $k = 1$ then $a_1\sigma(u) = 0 \ \forall u \in K$, so $a_1 = 0$ (since $\sigma_1(u) \neq 0$ unless $u = 0$), which is a contradiction. Since $\sigma_1 \neq \sigma_k$, $\exists c \in F$ s.t. $\sigma_1(c) \neq \sigma_k(c)$. Then for all $u \in F$,

$$\begin{aligned} 0 &= a_1\sigma_1(cu) + \cdots + a_k\sigma_k(cu) \\ &= a_1\sigma_1(c)\sigma_1(u) + \cdots + a_k\sigma_k(c)\sigma_k(u) \end{aligned} \tag{2}$$

Combining (1) and (2), for all $u \in F$,

$$a_2(\sigma_2(c) - \sigma_1(c))\sigma_2(u) + \cdots + a_k(\sigma_k(c) - \sigma_1(c))\sigma_k(u) = 0$$

$a_k \neq 0$ and $\sigma_k(c) - \sigma_1(c) \neq 0$ so the last coefficient is nonzero. So this is a relation among $\sigma_1, \ldots, \sigma_n$ having fewer than k terms, which is a contradiction. Thus, $\sigma_1, \ldots, \sigma_k$ are lin. indep. □

Theorem 3.8.3. *Let K be a field. Let $S = \{\sigma_\alpha\}$ be a set of automorphisms of K. Let*

$$F = \{x \in K \mid \sigma(x) = x \ \forall \sigma \in S\}.$$

Then F is a field.

F is called the **fixed field** of S in K, written $F = K^S$.

Proof. Suppose $a, b \in F$. Then $\forall \sigma \in S$,

$$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b.$$

$\therefore a + b \in F$. Similarly, $a - b, ab \in F$ and if $b \neq 0$, $\frac{a}{b} \in F$. □

Notation: Suppose $F \subset K$. Set

$$G(K, F) := \{\sigma \in \mathrm{Aut}(K) \mid \sigma(\alpha) = \alpha \ \forall \alpha \in F\}.$$

$G(K, F)$ forms a subgroup of $\mathrm{Aut}(K)$.

This gives us two functors:

$$\begin{array}{c}\text{Extension of fields} \rightsquigarrow \text{Subgroup of automorphisms of larger field} \\ F \subset K \rightsquigarrow G(K, F)\end{array}$$

and

$$\begin{array}{c}\text{Field, subgroup of its automorphisms} \rightsquigarrow \text{Extension of fields} \\ K, G \rightsquigarrow K^G \subset K\end{array}$$

Are these inverse processes? In general, no. Given $F \subset K$,

$$G(K, F) = \{\sigma \in K \mid \sigma(x) = x \forall x \in F\}$$

$\therefore K^{G(K,F)} = \{x \in K \mid \sigma(x) = x \forall \sigma \in G(K, F)\} \supset F$. But $K^{G(K,F)}$ can be strictly larger than F.

Example 3.8.4.

1. *$K = \mathbb{C}$, $F = \mathbb{R}$. Let $\sigma \in G(\mathbb{C}, \mathbb{R})$. $\sigma(x) = x \ \forall x \in \mathbb{R}$. So σ is determined by $\sigma(i)$.*

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1.$$

$\therefore \sigma(i) = \pm i$. So there are two elts. in $G(\mathbb{C}, \mathbb{R})$:

$$\begin{aligned} \sigma_1(i) = i \Rightarrow \ \sigma_1(a + bi) = a + bi \quad & \textit{identity of } G(\mathbb{C}, \mathbb{R}), \\ \sigma_2(i) = -i \Rightarrow \ \sigma_2(a + bi) = a - bi \quad & \textit{complex conjugation.} \end{aligned}$$

$\therefore G(\mathbb{C},\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Conversely,

$$\begin{aligned}\mathbb{C}^{G(\mathbb{C},\mathbb{R})} &= \{z \in \mathbb{C} \mid \sigma(z) = z \ \forall \sigma \in G(\mathbb{C},\mathbb{R})\} \\ &= \{z \in \mathbb{C} \mid z = \sigma_1(z) = z \text{ and } \overline{z} = \sigma_2(z) = z\} \\ &= \mathbb{R}\end{aligned}$$

In this case, we get our starting field back.

2. $F = \mathbb{Q}$, $K = \mathbb{Q}(a)$ *where* $a = 2^{\frac{1}{3}}$. *Let* $\sigma \in G(K,F)$. *Since* $\sigma(x) = x \ \forall x \in \mathbb{Q}$, σ *is determined by* $\sigma(a)$.

$$\sigma(a)^3 = \sigma(a^3) = \sigma(2) = 2,$$

so $\sigma(a)$ *is a cube root of* 2. *Since* $\mathbb{Q}(a)$ *contains only real numbers, it contains only one cube root of* 2, *namely a. So* $\sigma(a) = a$ *and* σ *is the identity. Thus,*

$$G(\mathbb{Q}(2^{\frac{1}{3}}),\mathbb{Q}) = 1.$$

$\therefore \mathbb{Q}(2^{\frac{1}{3}})^{G(\mathbb{Q}(2^{\frac{1}{3}}),\mathbb{Q})} = \mathbb{Q}(2^{\frac{1}{3}})$, *which is strictly larger than* $\mathbb{Q}$.

Let $f(x) \in F[x]$ and let $G = G(K,F)$ where K is the splitting field of $f(x)$. Let $\alpha_1,\ldots,\alpha_n \in K$ be the roots of

$$f(x) = c_0 + c_1x + \cdots + c_nx^n \quad (c_j \in F).$$

Let $\sigma \in G(K,F)$, so $\sigma(c_j) = c_j$. Then

$$\begin{aligned}f(\sigma(\alpha_i)) &= c_0 + c_1\sigma(\alpha_i) + \cdots + c_n(\sigma(\alpha_i))^n \\ &= \sigma(c_0 + c_1x + \cdots + c_nx^n) \\ &= \sigma(f(\alpha_i)) = \sigma(0) = 0.\end{aligned}$$

$\therefore \sigma(\alpha_i)$ is also a root of $f(x)$, ie. $\sigma(\alpha_i) = \alpha_{i'}$ for some $i' = 1,\ldots,n$. If $i \neq j$ then $\sigma(\alpha_i) \neq \sigma(\alpha_j)$, since σ is (1-1). So σ permutes the roots of $f(x)$. This map

$$\sigma \mapsto \sigma|_{\{\alpha_1,\ldots,\alpha_n\}}$$

is a group homomorphism $G \hookrightarrow S_n$.

Theorem 3.8.5. $|G(K,F)| \leq [K:F]$.

Proof. Let $[K : F] = n$ and let $u_1, \ldots, u_n$ be a basis for K over F. Suppose $G(K, F)$ has $n+1$ elements $\sigma_1, \ldots, \sigma_{n+1}$. Consider the system of equations

$$\begin{aligned}
\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \cdots + \sigma_{n+1}(u_1)x_{n+1} &= 0 \\
\sigma_1(u_2)x_1 + \sigma_2(u_2)x_2 + \cdots + \sigma_{n+1}(u_2)x_{n+1} &= 0 \\
&\vdots \\
\sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \cdots + \sigma_{n+1}(u_n)x_{n+1} &= 0.
\end{aligned}$$

This consists of n equations and $n+1$ variables, so $\exists$ a solution

$$x_1 = a_1,\ x_2 = a_2,\ \ldots,\ x_{n+1} = a_{n+1},$$

with not all $a_j = 0$. So, for all $j = 1, \ldots, n$,

$$a_1\sigma_1(u_j) + a_2\sigma_2(u_j) + \cdots + a_{n+1}\sigma_{n+1}(u_j) = 0.$$

Since $u_1, \ldots, u_n$ form a basis,

$$(a_1\sigma_1 + \cdots + a_{n+1}\sigma_{n+1})(t) = 0 \quad \forall t \in K.$$

But then $\sigma_1, \ldots, \sigma_{n+1}$ are linearly dependent in $\hom_{\text{abel. grps.}}(F, F)$, contradicting an earlier theorem.

Hence, $G(K, F)$ does not have $n+1$ elements, ie. $|G(K, F)| \leq [K : F]$. □

3.9 Elementary Symmetric Polynomials

Let F be a field.
Notation:

$$\begin{aligned} F(x_1, \ldots, x_n) &:= \text{ field of fractions of } F[x_1, \ldots, x_n] \\ &= \left\{ \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} \;\middle|\; p, q \in F[x_1, \ldots, x_n], q \neq 0 \right\} \end{aligned}$$

This is called the field of **rational functions** in n variables over F.

Let $K = F(x_1, \ldots, x_n)$. Given $\sigma \in S_n$, setting $\tilde{\sigma}(x_j) = x_{\sigma(j)}$ and $\tilde{\sigma}(a) = a \; \forall a \in F$ determines an automorphism of K s.t.

$$\sigma \in G(K, F) \subset \mathrm{Aut}(K).$$

In this way, S_n becomes a subgroup of $\mathrm{Aut}(K)$.

Let $S = K^{S_n}$. S is called the field of **symmetric rational functions** in n variables over F, and $S \cap F[x_1, \ldots, x_n]$ is called the ring of **symmetric polynomials** in n variables over F.

Definition 3.9.1. *Let*

$$s(t) = (t + x_1)(t + x_2) \cdots (t + x_n) \in F[x_1, \ldots, x_n][t].$$

*For $k = 1, \ldots, n$, the coefficient of t^{n-k} in $s(t)$ is called the k^{th} **elementary symmetric polynomial** in n variables, denoted $s_k(x_1, \ldots, x_n)$.*

For example:

$$\begin{aligned} s_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n \\ s_2(x_1, \ldots, x_n) &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots x_{n-1}x_n \\ s_3(x_1, \ldots, x_n) &= x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n \\ s_n(x_1, \ldots, x_n) &= x_1 \cdots x_n \end{aligned}$$

In general,

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Theorem 3.9.2.

1. $S = F(s_1, \ldots, s_n)$.
2. $[F(x_1, \ldots, x_n) : S] = n!$.

3. $G(F(x_1, \ldots, x_n), S) = S_n$.

4. $F(x_1, \ldots, x_n)$ *is the splitting field of* $s(t)$ *over* S.

Proof. $\sigma(s_k) = s_k \ \forall \sigma \in S_n$, so $F(s_1, \ldots, s_n) \subset S$. Conversely, $S_n \subset G(F(x_1, \ldots, x_n), S)$, so

$$[F(x_1, \ldots, x_n) : S] \geq |G(F(x_1, \ldots, x_n), S)| \geq |S_n| = n!.$$

$\therefore$ To show 1, 2 and 3, it suffices to show

$$[F(x_1, \ldots, x_n) : F(s_1, \ldots s_n)] \leq n!$$

since this simultaneously shows

$$[S : F(s_1, \ldots s_n)] = 1 \Rightarrow \ 1.$$

and

$$[F(x_1, \ldots, x_n) : S] = n! \Rightarrow \ 2.$$

and

$$|G(F(x_1, \ldots, x_n), S)| = n! \Rightarrow \ 3.$$

The polynomial

$$s(t) = (t + x_1)(t + x_2) \cdots (t + x_n)$$

factors linearly as shown in $F(x_1, \ldots, x_n)$. But its coefficients are $s_1, \ldots, s_n$, which lie in S. $s(t)$ cannot split in any proper subfield of $F(x_1, \ldots, x_n)$ since its roots are $-x_1, \ldots, -x_n$.

So $F(x_1, \ldots, x_n)$ is the splitting field of $s(t)$ over $F(s_1, \ldots, s_n)$. By an earlier corollary, the degree fo a splitting field extension of a polynomial of degree n is at most $n!$. Hence,

$$[F(x_1, \ldots, x_n) : F(s_1, \ldots, s_n)] \leq n!.$$

□

3.10 The Galois Group

Let $F \subset K$ be a separable finite extension of fields. We observed earlier that $F \subset K^{G(K,F)}$.

Definition 3.10.1. *K is called a **normal extension** (or **Galois extension**) of F if $F = K^{G(K,F)}$.*

eg. $\mathbb{R} \subset \mathbb{C}$ is normal, $\mathbb{Q} \subset \mathbb{Q}(2^{\frac{1}{3}})$ is not.

Theorem 3.10.2. *Let $F \subset K$ be a normal extension and let H be a subgroup of $G(K, F)$. Then*

1. $[K : K^H] = |H|$.
2. $H = G(K, K^H)$.

Corollary 3.10.3. *If $F \subset K$ is normal then $[K : F] = |G(K, F)|$.*

Proof of corollary. Let $H = G(K, F)$. Then

$$[K : F] = [K : K^{G(K,F)}] = |G(K, F)|.$$

□

Proof of theorem. $\forall \sigma \in H, x \in K^H$, $\sigma(x) = x$. So $H \subset G(K, K^H)$. Thus

$$[K : K^H] \geq |G(K, K^H)| \geq |H|.$$

Since $F \subset K$ is separable, so is $K^H \subset K$. Hence, $\exists a \in K$ s.t. $K = K^H(a)$.

By an earlier theorem, the min. poly. of a has degree $[K : K^H]$. Let

$$H = \{\sigma_1, \ldots, \sigma_h\},$$

where $\sigma_1 = 1$. Let

$$s_1(x_1, \ldots, x_h), \ldots, s_h(x_1, \ldots, x_h)$$

be the elementary symmetric polynomials in h variables. Let

$$\alpha_j = s_j(\sigma_1(a), \sigma_2(a), \ldots, \sigma_h(a)) \in K.$$

Let

$$p(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \ldots (x - \sigma_h(a)) = x^h - \alpha_1 x^{h-1} + \alpha_2 x^{h-2} + \cdots + (-1)^h \alpha_h \in K[x].$$

In any group, left multiplication by any element permutes the elements of the group. By construction, each α_j is invariant under permutations of the σ's. So for all j, $\sigma(\alpha_j) = \alpha_j$ $\forall \sigma \in H$, so $\alpha_j \in K^H$. Hence $p(x) \in K^H[x]$. Since $a = \sigma_1(a)$ is a root of $p(x)$,

$$|H| = h = \deg p(x) \geq \deg(\text{min. poly. of } a \text{ over } K^H) = [K : K^H].$$

$\therefore |H| = |G(K, K^H)| = [K : K^H]$, showing 1, and also $H \subset G(K, K^H)$, showing 2. □

Theorem 3.10.4. *Suppose K is separable over F. Then $F \subset K$ is a normal extension $\iff$ K is the splitting field of some polynomial in F.*

Proof.

$\Rightarrow$: Suppose $F \subset K$ is a normal extension. $K = F(a)$ for some $a \in K$. Let

$$G(K, F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\},$$

where $\sigma_1 = 1$. Let

$$\begin{aligned} p(x) &= (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a)) \\ &= x^n - \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + (-1)^n \alpha_n, \end{aligned}$$

where $\alpha_j = s_j(\sigma_1(a), \ldots, \sigma_n(j)) \in K$. As in the preceding proof, $\sigma(\alpha_j) = \alpha_j \ \forall \sigma \in G(K, F)$, so

$$\alpha_j \in K^{G(K,F)} = F,$$

by normality.

So $p(x) \in F[x]$ and $p(x)$ splits in K. $a = \sigma_1(a)$ is a root of $p(x)$. By defn. of $F(a)$, a lies in no proper subfield of $K = F(a)$ which contains F. So $p(x)$ does not split in any subfield of K. Thus, K is the splitting field of $p(x)$.

$\Leftarrow$: Let K be the splitting field of some $f(x) \in F[x]$.

Lemma 3.10.5. *Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ and let $\alpha_1, \ldots, \alpha_r \in K$ be the roots of $p(x)$. Then $\forall j = 1, \ldots, r$, $\exists \sigma_j \in G(K, F)$ s.t. $\sigma_j(\alpha_1) = \alpha_j$.*

Proof of lemma. By Theorem 3.3.13, $\exists$ an isomorphism

$$\tau_j : F(\alpha_1) \overset{\cong}{\longmapsto} F(\alpha_j)$$

s.t. $\tau_j(\alpha_1) = \alpha_j$ and $\tau_j(z) = z \ \forall z \in F$. Hence, $\tau_j(f(x)) = f(x)$.

K can be regarded as the splitting field of $f(x)$ over both $F(\alpha_1)$ and $F(\alpha_j)$. So by Theorem 3.3.15, τ_j can be extended to

$$\sigma_j : K \overset{\cong}{\longmapsto} K.$$

Since σ_j extends τ_j, $\sigma_j \in G(K, F)$ and $\sigma_j(\alpha_1) = \alpha_j$, as required. □

Proof of theorem (continued). Assume by induction that if K_1 is the splitting field of some polynomial $f_1 \in F_1[x]$ and $[K_1 : F_1] < [K : F]$ then K_1 is normal over F_1. If $[K_1 : F_1] = 1$ then $K_1 = F_1$ is normal over F_1, to start induction.

So suppose $[K : F] > 1$. Then $f(x)$ has a non-linear irreducible factor $p(x)$. Let

$$\deg p(x) = r > 1.$$

Let $\alpha_1, \ldots, \alpha_r \in K$ be the roots of $p(x)$. Regarding K as the splitting field of $f(x)$ over $F(\alpha_1)$, induction implies that K is a normal extension of $F(\alpha_1)$. Show $K^{G(K,F)} = F$.

$F \subset F(\alpha_1)$, so $G(K, F(\alpha_1)) \subset G(K, F)$. ie. $\sigma \in G(K, F(\alpha_1)) \Rightarrow \ \sigma(z) = z \ \forall z \in F(\alpha_1)$, and in particular, $\sigma(z) = z \ \forall z \in F$. Thus,

$$K^{G(K,F)} \subset K^{G(K,F(\alpha_1))} = F(\alpha_1),$$

because $F(\alpha_1) \in K$ is normal.

Let $z \in K^{G(K,F)}$. We must show $z \in F$. Since $z \in F(\alpha_1)$,

$$z = \lambda_0 + \lambda_1\alpha_1 + \cdots + \lambda_{r-1}\alpha^{r-1},$$

for some $\lambda_0, \ldots, \lambda_{r-1} \in F$. For $j = 1, \ldots, r$, choose $\sigma_j \in G(K, F)$ s.t. $\sigma(\alpha_1) = \alpha_j$. Then

$$z = \sigma_j(z) = \lambda_0 + \lambda_1\alpha_j + \cdots + \lambda_{r-1}\alpha_j^{r-1}$$

Let

$$q(x) = \lambda_{r-1}x^{r-1} + \cdots + \lambda_1 x + (\lambda_0 - z) \in K[x]$$

Then α_j is a root of $q(x) \ \forall j = 1, \ldots, r$. But $\deg q(x) \leq r - 1$ and $\alpha_1, \ldots, \alpha_r$ are distinct. This is a contradiction unless all coefficients of $q(x)$ are zero. In particular, $z = \lambda_0 \in F$.

□

Definition 3.10.6. *Let $f(x) \in F[x]$. Let K be the splitting field of f over F and suppose that K is separable over F. The **Galois group** of $f(x)$ over F is $G(K, F)$. This will sometimes be denoted* $\mathrm{Gal}(f(x))$.

Theorem 3.10.7 (Fundamental Theorem of Galois Theory)**.** *Let $f(x) \in F$. Let $K \supset F$ be the splitting field of $f(x)$ over F. Suppose K is separable over F and let $G = G(K, F)$ be the Galois group of $f(x)$ over F. Then the associations*

$$M \rightsquigarrow G(K, M)$$
$$K^H \reflectbox{$\rightsquigarrow$} H$$

set up a bijection between fields M s.t. $F \subset M \subset K$ and subgroups of G. It has the following properties:

1. $M = K^{G(K,M)}$.
2. $H = G(K, K^H)$.
3. $[K : M] = |G(K, M)|$, *and* $[M : F] = G : G(K, M)$ *(the index of the subgroup* $G(K, M)$ *in* G*).*
4. M *is a normal extension of* $F \iff G(K, M)$ *is a normal subgroup of* G.
5. *If* M *is a normal extension of* F *then* $G(M, F) \cong G/G(K, M)$.

Proof.

1. K is the splitting field of $f(x)$ over F, so F can be regarded as the splitting field of $f(x)$ over M. So $M \subset K$ is normal, ie. $M = K^{G(K,M)}$.
2. This is just Theorem 3.10.2. 1 and 2 say that the associations are inverse bijections.
3. $$\begin{aligned} |G(K, M)| &= [K : K^{G(K,M)}] \quad \text{by Theorem 3.10.2} \\ &= [K : M] \quad \text{by 1.} \end{aligned}$$
   and
   $$[M : F] = \frac{[K : F]}{[K : M]} = \frac{|G(K, F)|}{|G(K, M)|} = G : G(K, M).$$
4. **Lemma 3.10.8.** M *is normal* $\iff \sigma(M) \subset M \; \forall \sigma \in G$.

   Proof of lemma.

   $\Rightarrow$: Suppose M is normal. Let $\sigma \in G$. Let $q(x) \in F[x]$ be a polynomial whose splitting field is M. So in M,
   $$q(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r).$$
   By an earlier proposition, $M = F(\alpha_1, \alpha_2, \ldots, \alpha_r)$. Since $\sigma \in G$,
   $$q(\sigma(\alpha_j)) = \sigma(q(\alpha_j)) = \sigma(0) = 0.$$
   $\therefore \sigma(\alpha_j)$ is a root of $q(x)$. But M contains the full set of roots of $q(x)$, so $\sigma(\alpha_j) \in M$. Thus, $\sigma(M) \subset M$.

$\Leftarrow$: Suppose $\sigma(M) \subset M \ \forall \sigma \in G$. Let $z \in M^{G(M,F)}$, and check that $z \in F$. Let $\sigma \in G$. Since $\sigma(M) \subset M$, $\sigma|_M \in G(M,F)$. So,

$$\sigma(z) = \sigma|_M(z) = z,$$

since $z \in M^{G(M,F)}$. So $z \in M^G \subset K^G = F$.

□

Proof of 4.

$\Rightarrow$: Suppose M is a normal extension of F. Let $\sigma \in G, \tau \in G(K,M)$. Then $\forall m \in M$,

$$\begin{aligned}\sigma^{-1}\tau\sigma(m) &= \sigma^{-1}\tau(\sigma(m)) \\ &= \sigma^{-1}\sigma(m), \quad \text{since } \sigma(m) \in M \text{ and } \tau|_M = \mathrm{id} \\ &= m.\end{aligned}$$

$\therefore \sigma^{-1}\tau\sigma \in G(K,M)$. Hence $G(K,M)$ is a normal subgroup of G.

$\Leftarrow$: Suppose $G(K,M)$ is a normal subgroup of G. Let $\sigma \in G, z \in M$. Then $\forall \tau \in G(K,M)$, $\sigma^{-1}\tau\sigma \in G(K,M)$, so

$$\sigma^{-1}\tau\sigma(z) = z.$$

$\therefore \tau\sigma(z) = \sigma(z)$. Thus $\sigma(z) \in K^{G(K,M)} = M$ (by 1). So $\sigma(M) \subset M$ and M is normal over F by the lemma.

5. Suppose M is normal over F. Given $\sigma \in G(K,F)$, define $\psi(\sigma) = \sigma|_M$. By the lemma,

$$\sigma(M) \subset M,$$

so $\psi(\sigma) \in G(M,F)$. If $\sigma \in \ker\psi$ then $\sigma|_M = \mathrm{id}_M$, ie. $\sigma \in G(K,M)$. Hence, $\ker\psi = G(K,M)$. So by 1st isomorphism theorem,

$$G/G(K,M) = G/\ker\psi \cong \mathrm{Im}\psi \subset G(M,F).$$

But $|G/G(K,M)| = [M:F] = |G(M,F)|$, so

$$G/G(K,M) \cong G(M,F).$$

□

Theorem 3.10.9. *Let $F \subset K$ be an extension field. Let $f(x) \in F[x]$. Then the Galois group of $f(x)$ over K is isomorphic to a subgroup of the Galois group of $f(x)$ over F.*

Proof. Let L be the splitting field of $f(x)$ over K and E the splitting field of $f(x)$ over F. Since $f(x)$ splits in L, $E \subset L$. Let $r_1, \ldots, r_n \in E$ be the roots of $f(x)$.

For $\sigma \in G(L, K)$, σ is determined by its action on $r_1, \ldots, r_k$. Define $\psi : G(L, K) \mapsto G(E, F)$ by $\psi(\sigma) = \sigma|_E$. If $\psi(\sigma) = \psi(\tau)$ then $\sigma|_E = \tau|_E$, so

$$\sigma(r_j) = \tau(r_j) \quad \forall j.$$

$\therefore \sigma = \tau$. Hence ψ is a monomorphism. □

3.11 Constructions with Ruler and Compass

Let $S \subset \mathbb{C} \cong \mathbb{R}^2$ be a finite subset. Let

$$S' := \{z \in \mathbb{C} \mid z \text{ can be constructed from the points of } S \text{ using a ruler and compass}\}.$$

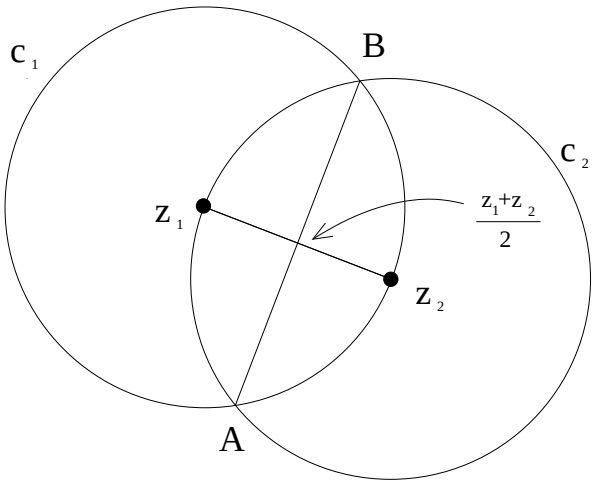
More precisely:
Let $S_0 = S$. Using a ruler and compass, we can join pts. in S_0 with lines or can construct circles centred at a point in S_0 and passing through another point in S_0. Let $\tilde{S}_0$ be the set of points which are the intersections of these lines and circles.
Let $S_1 = S_0 \cup \tilde{S}_0$, $S_2 = S_1 \cup \tilde{S}_1, \ldots, S_n = S_{n-1} \cup \tilde{S}_{n-1}$. Then let

$$S' = \bigcup_n S_n.$$

Let $P_0 = 0 = (0,0), P_1 = 1 = (1,0)$. Let $F = \{P_0, P_1\}'$. We say z is **constructible** if $z \in F$. Show F is a field.

Proposition 3.11.1. *If $z_1, z_2 \in S'$ then $\frac{z_1+z_2}{2} \in S'$.*

Proof.



Let $c_1 := C_{z_1}(z_2)$, the circle centred at z_1 through z_2, and let $c_2 := C_{z_2}(z_1)$. Let A, B be the two intersection points of c_1 and c_2. Then $L(A,B)$, the line through A and B, intersects $L(z_1, z_2)$ at $\frac{z_1+z_2}{2}$. □

Proposition 3.11.2. *If $z_1, z_2 \in F$ then $z_1 + z_2 \in F$.*

Proof. $C_{\frac{z_1+z_2}{2}}(0)$ meets $L\left(0, \frac{z_1+z_2}{2}\right)$ at $z_1 + z_2$ (and 0). □

Proposition 3.11.3. *If $z \in F$ then $-z \in F$.*

Proof. Intersect $L(0,z)$ with $C_0(z)$. □

Proposition 3.11.4. $z = (x,y) \in F \iff (x,0) \in F$ *and* $(0,y) \in F$.

Proof.

$\Rightarrow$: Suppose $z = (x,y) \in F$. $C_z(0)$ meets $L(0,P_1)$ at $(2x,0)$, so $(2x,0) \in F$. By Prop. 3.11.1, $(x,0) \in F$. Hence also,

$$(0,y) = (x,y) - (x,0) \in F.$$

$\Leftarrow$: If $(x,0),(0,y) \in F$ then by Prop. 3.11.2,

$$(x,y) = (x,0) + (0,y) \in F.$$

□

Let

$$\mathcal{L} := \{\text{lines joining two points in } F\}.$$

Proposition 3.11.5. *Let $L \in \mathcal{L}, A \in F$. Then the line parallel to L through A lies in $\mathcal{L}$.*

Proof. Let $P, Q \in F$ be distinct points lying on L. Let

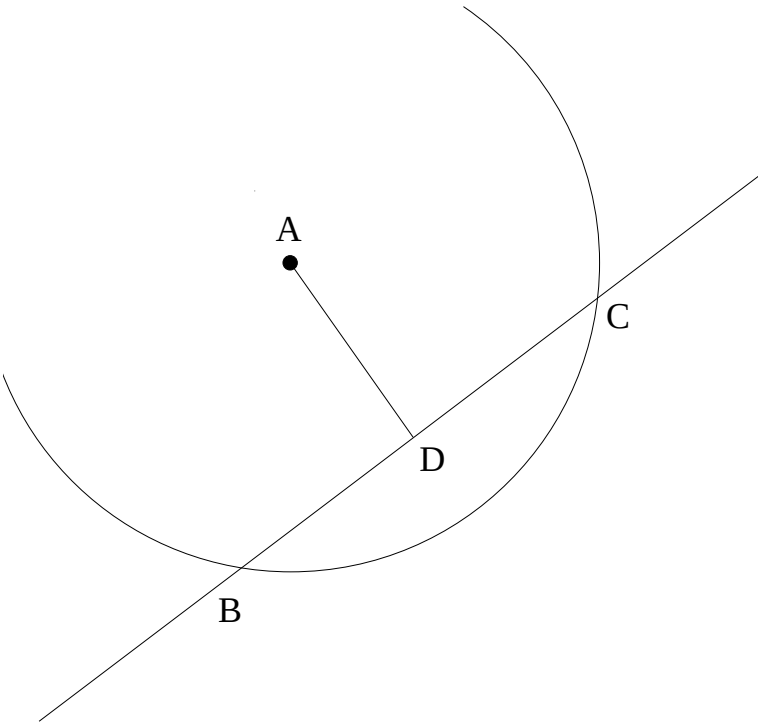
$$R = P - Q + A \in F.$$

Then the line parallel to L through A is $L(A,R)$. □

Proposition 3.11.6. *Let $L \in \mathcal{L}, A \in F$. Then the line through A perpendicular to L lies in $\mathcal{L}$.*

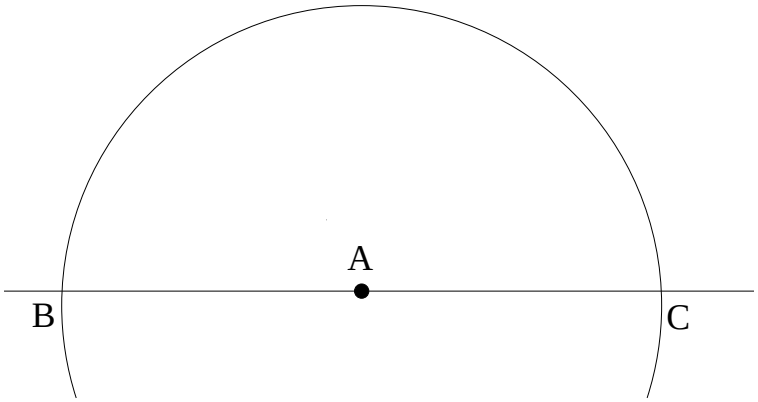
Proof.

Case 1: $A \notin L$. Let C be the other point where $C_A(B)$ meets L and let $D = \frac{B+C}{2}$. (If $C_A(B)$ happens to be tangent to L at B then let $D = B$).



Then $D \in F$ and $L(A, D)$ is the line perependicular to BC through A.

Case 2: $A \in L$. Since L has at least two points of F, let $A \neq B \in L$. Let C be the other point where $C_A(B)$ meets L.



Then $A = \frac{B+C}{2}$ and the construction of Prop. 3.11.1 produces the line through A perpendicular to L.

□

Proposition 3.11.7. *Let $z = re^{i\theta}$. Then $z \in F \iff r \in F$ and $e^{i\theta} \in F$.*

Proof.

⇒: Suppose $z \in F$. $C_0(z)$ meets $L(0, P_1)$ at $(r, 0)$, ie. $r \in F$. $e^{i\theta}$ is the point where $L(0, re^{i\theta})$ crosses $C_0(P_1)$. Hence $e^{i\theta} \in F$.

⇐: Let $r \in F$ and $e^{i\theta} \in F$. Then $re^{i\theta}$ is the point where $L(0, e^{i\theta})$ meets the circle centred at 0 through $(r, 0)$.

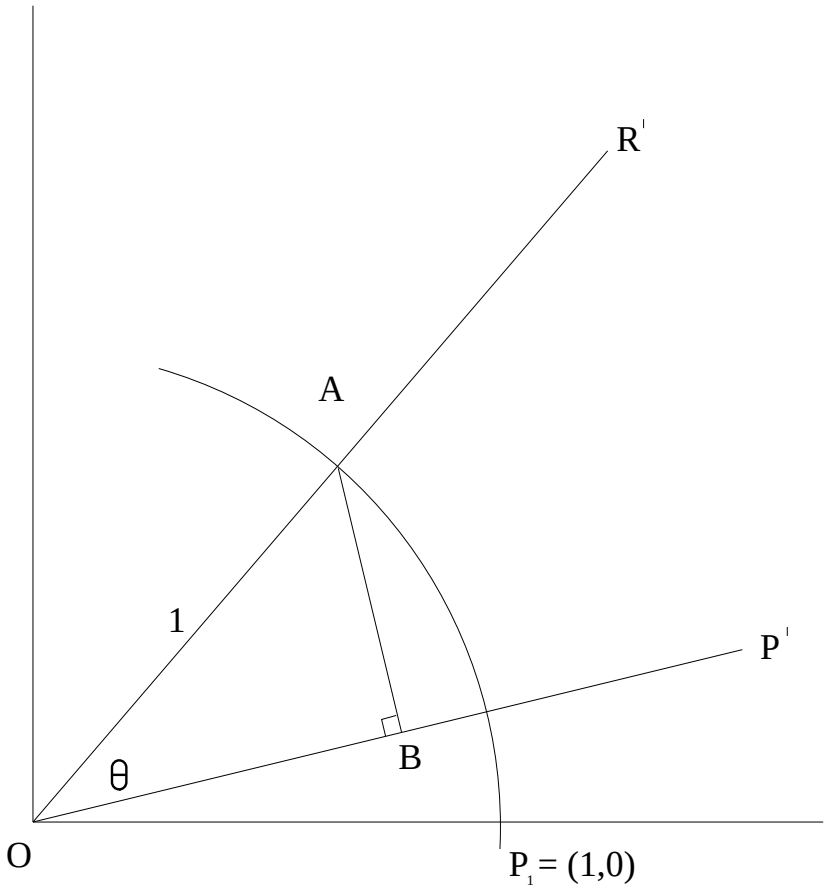
□

Proposition 3.11.8. *$\exists P, Q, R \in F$ s.t. $\angle PQR = \theta \iff e^{i\theta} \in F$.*

Proof.

⇒: Suppose $P, Q, R \in F$ s.t. $\angle PQR = \theta$. Let

$$P' = P - Q, R' = R - Q \in F.$$



Let A be the point where $C_0(P_1)$ meets $L(0, R')$. Let B be the point where the perpendicular to $L(0, P')$ through A meets $L(O, P')$. Then

$$\cos\theta = |0B| \in F.$$

Also, letting $z = A - B$,

$$\sin\theta = |AB| = |z| \in F.$$

Then the y-axis is in $\mathcal{L}$ by Prop. 3.11.6, and $i\sin\theta$ is the point where $C_0(\sin\theta)$ meets the y-axis, whence $i\sin\theta \in F$. So

$$e^{i\theta} = \cos\theta + i\sin\theta \in F.$$

$\Leftarrow$: Suppose $e^{i\theta} \in F$. Let

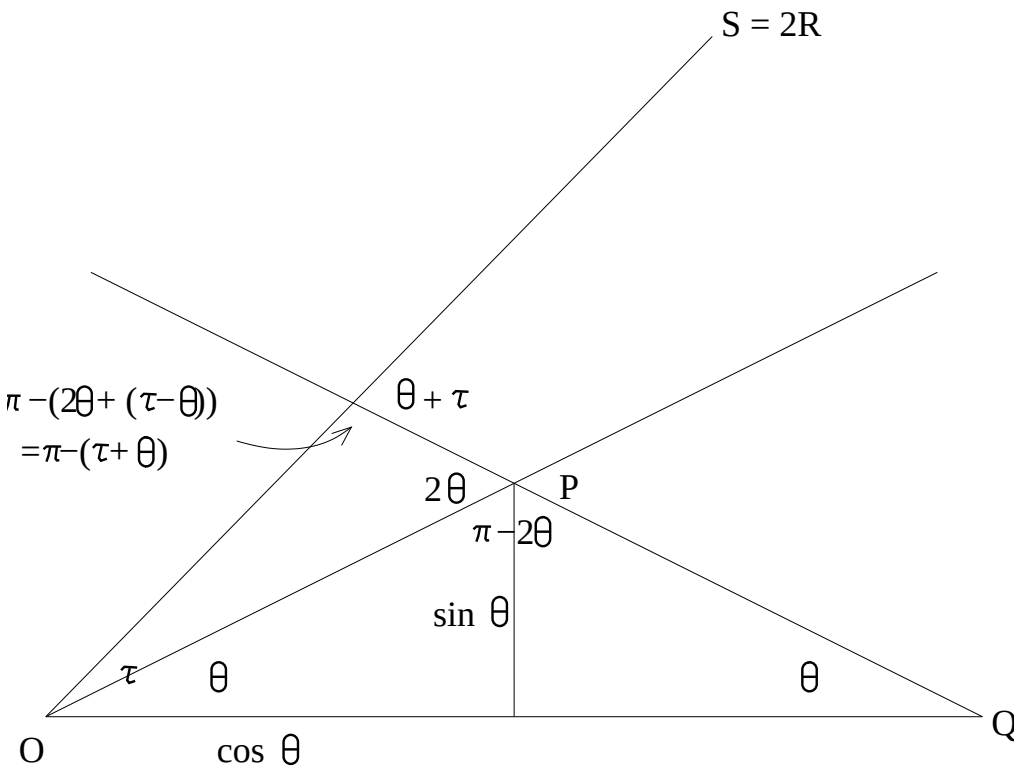
$$P = (0, 1), \quad Q = 0, \quad R = e^{i\theta} = (\cos\theta, \sin\theta).$$

Then $\angle PQR = \theta$.

□

Proposition 3.11.9. *Let* $(\cos\theta, \sin\theta) \in F$ *and* $(\cos\tau, \sin\tau) \in F$. *Then* $(\cos(\theta + \tau), \sin(\theta + \tau)) \in F$.

Proof.



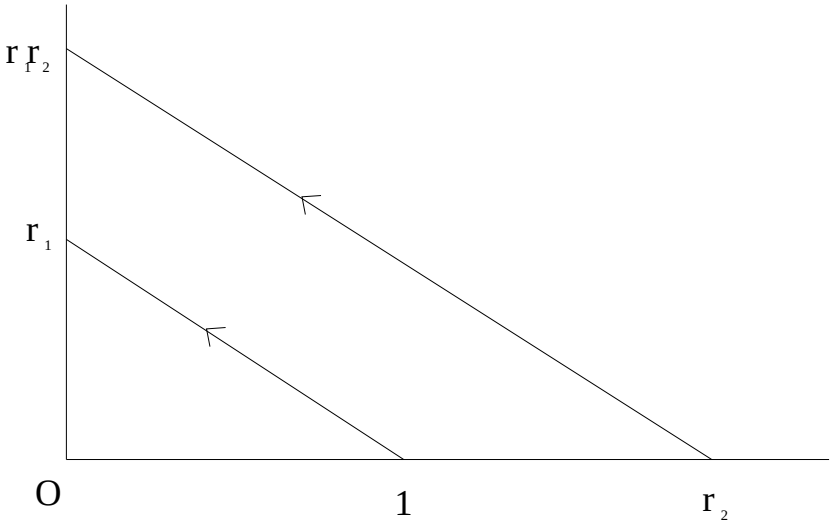
Let $P = (\cos\theta, \sin\theta)$, so $(\cos\theta, 0) \in F$. Let $Q = (2\cos\theta, 0) \in F$. Let R be the point where $L(Q, P)$ meets the line joining 0 to $(\cos\tau, \sin\tau)$. Let $S = 2R$. Then $Q, R, S \in F$ and $\angle QRS = \theta + \tau$. So

$$(\cos(\theta + \tau), \sin(\theta + \tau)) \in F.$$

□

Proposition 3.11.10. *If $z_1, z_2 \in F$ then $z_1 z_2 \in F$.*

Proof. Let $z_1 = r_1 e^{i\theta_1}$, $z_2\ r_2 e^{i\theta_2}$. Then $z_1 \in F \Rightarrow (r_1, 0) \in F$ and $z_2 \in F \Rightarrow (r_2, 0) \in F$.



The line joining $(r_1, 0)$ to $(0, r_1 r_2)$ is parallel to that joining $(1, 0)$ to $(0, r_2)$, so it lies in $\mathcal{L}$. Hence, its intersection with the y-axis lies in F, ie. $(0, r_1 r_2) \in F$.

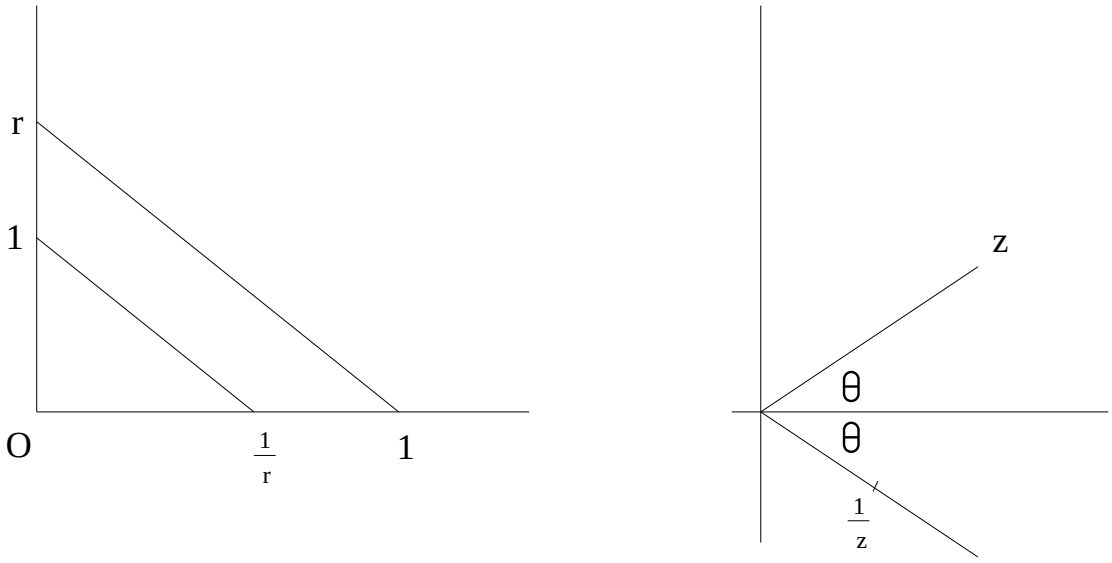
$z_1 \in F \Rightarrow (\cos\theta_1, \sin\theta_1) \in F$ and $z_2 \in F \Rightarrow (\cos\theta_2, \sin\theta_2) \in F$ by Prop. 3.11.7. So by Prop. 3.11.9,

$$P = (\cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2)) \in F.$$

$L(0, P)$ meets the circle centred at 0 through $(0, r_1 r_2)$ at $z_1 z_2$. □

Proposition 3.11.11. *If $z \in F$ then $\frac{1}{z} \in F$.*

Proof. Let $z = re^{i\theta}$.



As above, $z \in F \Rightarrow (0, r) \in F \Rightarrow$ the line joining $(1, 0)$ to $(0, r)$ lies in $\mathcal{L}$. So the line joining $(\frac{1}{r}, 0)$ to $(0, 1)$ lies in $\mathcal{L}$, and thus, $(\frac{1}{r}, 0) \in F$.

$e^{i\theta} \in F$, so by Props. 3.11.3 and 3.11.4, $e^{-i\theta} \in F$. By Prop. 3.11.10,

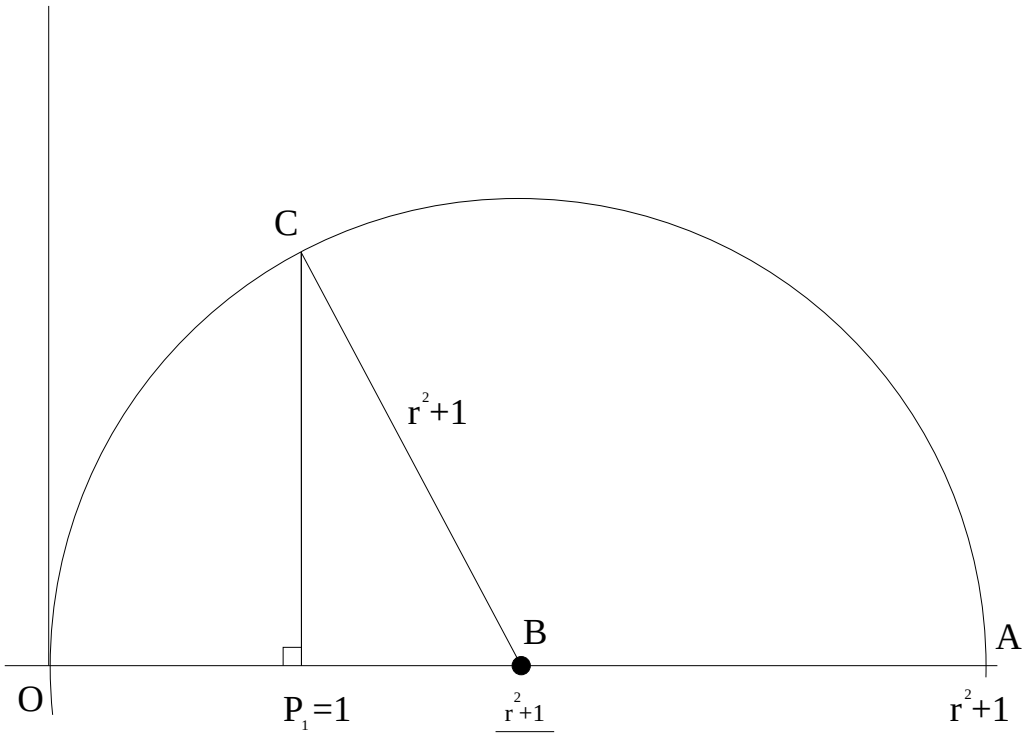
$$\frac{1}{z} = \frac{1}{r} e^{-i\theta} \in F.$$

□

Thus, F is a field.

Proposition 3.11.12. *If $z^2 \in F$ then $z \in F$.*

Proof. $z = \left(\frac{z+1}{2}\right)^2 - \left(\frac{z-1}{2}\right)^2$.



Let $z = re^{i\tau}$, so $z^2 = r^2e^{i2\tau} \in F$. Then $(r^2, 0) \in F$ so $A = (r^2, 0) + (1, 0) \in F$. Let $B = \frac{A}{2} \in F$. Let C be the point where $C_B(A)$ meets the perpendicular to $L(0, A)$ through $(1, 0)$. By Pythagoras,

$$|P_1C|^2 = |BC|^2 - |P_1B|^2 = \left(\frac{r+1}{2}\right)^2 - \left(\frac{r-1}{2}\right)^2.$$

$\therefore C = (1, r)$ so $r \in F$.

Let $\theta = 2\tau$. $r^2e^{2i\tau} \in F \Rightarrow e^{i2\tau} \in F$, ie. $Q = (\cos\theta, \sin\theta) \in F$. Let

$$\begin{aligned} S &= Q - P_1 \\ &= (\cos 2\tau - 1, \sin 2\tau) \\ &= (2\cos^2\tau, 2\cos\tau\sin\tau) \\ &= 2\cos\tau(\cos\tau, \sin\tau). \end{aligned}$$

So, if $\cos\tau \neq 0$ then $\angle P_1 0S = \tau$, ie. $L(0, S)$ bisects $\angle P_1 0Q$. If $\cos\tau = 0$ then $\tau = \pm\frac{\pi}{2}$ and it is obvious that a line with angle τ is in $\mathcal{L}$. The circle centred at 0 passing through $(r, 0)$ meets this line at $re^{i\tau} \in F$. □

Theorem 3.11.13. *F is the smallest subfield of $\mathbb{C}$ which is closed under square roots and complex conjugation.*

Proof. By earlier propositions, F is closed under square roots and complex conjugation. Conversely, let K be a subfield of $\mathbb{C}$ closed under square roots and complex conjugation. Since $S_0 = \{0, 1\} \in K$, if we can show that $K' = K$, it will follow that $F \subset K$.

Lemma 3.11.14. *The equation of a line joining two points in K can be written in the form*

$$ax + by = c$$

where $a, b, c \in K \cap \mathbb{R}$.

Proof. Let L join $P = (p_1, p_2)$ to $Q = (q_1, q_2)$, where $p_1, p_2, q_1, q_2 \in K \cap \mathbb{R}$. (Since K is closed under complex conjugation, it is clear that this can be done for any elements $P, Q \in K$). Then L has the equation

$$(q_1 - p_1)(y - p_2) = (q_2 - p_2)(x - p_1),$$

which has the desired form. □

Lemma 3.11.15. *The equation for a circle centred at a point of K passing through another point of K can be written in the form*

$$x^2 + y^2 + ax + by + c = 0$$

where $a, b, c \in K \cap \mathbb{R}$.

Proof. Let C be the circle centered at $P = (p_1, p_2)$ passing through $Q = (q_1, q_2)$., where $p_1, p_2, q_1, q_2 \in K \cap \mathbb{R}$. Then the radius of C is

$$r = \sqrt{(q_2 - p_q)^2 + (q_1 - p_1)^2} \in K \cap \mathbb{R}.$$

So C has the equation

$$(x - p_1)^2 + (y - p_2)^2 = r^2,$$

which has the desired form. □

Proof of Theorem (continued).

1. The intersection of $ax + by = c, a'x + b'y = c'$ is the solution of the simultaneous equations, which is given by a quotient of determinants involving a, b, c, a', b', c'. So the intersection is $z = (p, q)$ where $p, q \in K \cap \mathbb{R}$. Hence $z = p + iq \in K$.

2. The intersection(s) of $ax + by = c$ and $x^2 + y^2 + a'x + b'y + c' = 0$:

$$x^2 + \left(\frac{c - ax}{b}\right)^2 + a'x + b'\left(\frac{c - ax}{b}\right) + c' = 0.$$

(consider $b = 0$ separately: exercise). This is a quadratic, so if there is a solution then by quadratic formula, it lies in $K \cap \mathbb{R}$. Similarly, the solution for y lies in $K \cap \mathbb{R}$.

3. Intersection(s) of $x^2 + y^2 + ax + by + c = 0$ and $x^2 + y^2 + a'x + b'y + c' = 0$:
   By subtracting the equations, get

$$(a - a')x + (b - b')y + c - c' = 0$$

   so the intersection pts. are the same as that of the line $(a - a')x + (b - b')y + c - c' = 0$ and the circle $x^2 + y^2 + ax + by + c = 0$, which transposes into case 2.

□

Theorem 3.11.16. *If $z \in F$ then z is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of* 2.

Proof. By the last theorem, if $z \in F$ then we can create a field K s.t. $z \in K$ by a finite number of extensions, each of which adjoins the square root of some element. That is,

$$\mathbb{Q} \subset \mathbb{Q}(z) \subset K$$

where $\mathbb{Q} \subset K$ is a composition of some sequence of degree 2 extensions. So

$$[K : \mathbb{Q}] = 2^t$$

for some t, and $[\mathbb{Q}(z) : \mathbb{Q}]$ divides 2^t, so it is a power of 2. □

Example 3.11.17. *It is impossible by ruler and compass to trisect* $60°$.

Proof. Using earlier techniques, we can construct equilateral triangles and thus $\cos 60°, \sin 60° \in F$. If $60°$ could be trisected, then $\alpha = \cos 20°$ would be in F.

In general,

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

For $\theta = 20°$, $\cos 3\theta = \cos 60 = \frac{1}{2}$. So

$$\frac{1}{2} = 4\alpha^3 - 3\alpha$$

or

$$8\alpha^3 - 6\alpha - 1 = 0.$$

But $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$, so

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3,$$

which is not a power of 2. Hence $\alpha \notin F$. So $60°$ cannot be trisected using ruler and compass. □

Example 3.11.18. *It is impossible by ruler and compass to "double" the cube (ie. to construct a cube whose volume is twice that of a given cube). (Historically, this was called "duplicating" the cube).*

Proof. Suppose the volume of the original cube is 1. Then the length of the edge of the new cube is $2^{\frac{1}{3}}$, whose min. poly. is $x^3 - 2$. Since 3 is not a power of 2, $2^{\frac{1}{3}}$ is not constructible, so we cannot duplicate the cube. □

3.12 Solvability by Radicals

$g(x) = x^2 + bx + c \Rightarrow x = \frac{-b \pm \sqrt{b^2-4c}}{2}$. So if $b, c \in \mathbb{Q}$, then we can form the splitting field of $f(x)$ by adjoining to $\mathbb{Q}$ the square root of some elt. of $\mathbb{Q}$.

$g(x) = x^3 + ax^2 + bx + c$. We shall see, $\exists$ a formula where, by successively adding roots (cube roots and square roots) to our field, we can produce the splitting field of $g(x)$. $\exists$ a similar formula for quartics.

Given a field F and a polynomial $p(x) \in F[x]$, we say that $p(x)$ is **solvable by radicals** over F if we can find a sequence of fields satisfying:

$$\begin{aligned} F_0 &= F \\ F_1 &= F_0(w_1) \quad \text{where } w_1^{r_1} \in F_0 \text{ for some } r_1 \\ F_2 &= F_1(w_2) \quad \text{where } w_2^{r_2} \in F_1 \text{ for some } r_2 \\ &\vdots \\ F_n &= F_{n-1}(w_n) \quad \text{where } w_n^{r_n} \in F_{n-1} \text{ for some } r_n \end{aligned}$$

such that $p(x)$ splits in F_n. (We do not require that F_n be the splitting field of $p(x)$; it could be larger. Thus, F_n might not be normal.)

Let $F = K(a_1, \ldots, a_n)$ be the field of fractions in n variables. The general polynomial of degree n over K,

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

can be regarded as an elements of $F[x]$. Finding a "formula" involving roots for the general polynomial of degree n over K means showing that $p(x) \in F[x]$ is solvable by radicals. We shall show that that this is not true if $n \geq 5$.

Note: This does not mean that it is impossible for some specific 5^{th} degree polys. in $K[x]$ to be solvable by radicals.

Theorem 3.12.1. *Suppose* $\operatorname{char} F = 0$. *Let* $p(x) = x^n - 1 \in F[x]$. *Then* $F\left(e^{\frac{2\pi i}{n}}\right)$ *is the splitting field of* $p(x)$ *over* F, *and the Galois group of* $p(x)$ *over* F *is abelian.*

Proof. Let $w = e^{\frac{2\pi i}{n}}$. Then all roots of $p(x)$ are powers of w, so $F(w)$ is the splitting field for $p(x)$ over F.

Let $\sigma, \tau \in G = G(F(w), F)$. σ is determined by $\sigma(w)$, since $\sigma(f) = f \ \forall f \in F$. $\sigma(w)$ is a root of $x^n - 1$, so let

$$\sigma(w) = w^j, \quad \text{for some } j.$$

Similarly,

$$\tau(w) = w^k, \quad \text{for some } k.$$

So

$$\sigma\tau(w) = \sigma(w^k) = (\sigma(w))^k = (w^j)^k = w^{jk} = \tau\sigma(w).$$

ie. $\sigma\tau = \tau\sigma$. So G is abelian. □

Theorem 3.12.2. *Suppose* $\operatorname{char} F = 0$ *and suppose* $w = e^{\frac{2\pi i}{n}} \in F$. *Let* u *be a root of* $p(x) = x^n - a$ *lying in an extension field of* F. *Then* $F(u)$ *is the splitting field of* $p(x)$ *over* F *and the Galois group of* $x^n - a$ *over* F *is cyclic, with order dividing* n.

Proof. Let $F \subset K$ be an extension s.t. $u \in K$. Then the n roots of $x^n - a$ are

$$u, wu, w^2u, \ldots, w^{n-1}u,$$

which all lie in $F(u)$. So $F(u)$ is the splitting field of $p(x)$ over F.

Let $G = G(F(u), F)$. Let $\sigma \in G$. Then $\sigma(u)$ is a root of $p(x)$, so $\sigma(u) = w^j u$ for some j, and σ is determined by $\sigma(u)$. Define $\psi : G \mapsto \mathbb{Z}/n\mathbb{Z}$ by

$$\psi(\sigma) = j \quad \text{where } \sigma(u) = w^j u.$$

If $\psi(\tau) = k$ then

$$\sigma\tau(u) = \sigma(w^k u) = \sigma(w^k)\sigma(u) = w^k w^j u = w^{j+k} u.$$

$\therefore \psi(\sigma\tau) = j + k = \psi(\sigma) + \psi(\tau)$, so ψ is a group homomorphism. If $\psi(\sigma) = \psi(\tau)$ then $\sigma(u) = \sigma(\tau)$ and thus $\sigma = \tau$. Hence ψ is a monomorphism. Thus,

$$G \cong \text{subgroup of a cyclic group of order } n,$$

so G is cyclic with order dividing n. □

Theorem 3.12.3. *Let* p *be prime. Suppose* $\exists p$ *distinct elts.* $z_1, \ldots, z_n \in F$ *s.t.*

$$z_j^p = 1 \quad \forall j.$$

Let $F \subset E$ *be normal s.t.* $G = G(E, F)$ *is cyclic of order* p. *Then* $E = F(u)$ *where* $u^p \in F$.

Proof. Let $c \in E - F$. Since $[E : F] = |G| = p$, there are no fields lying strictly between F and E, so $E = F(c)$. Let σ be a generator of G. Let

$$c_1 = c, c_2 = \sigma(c), c_3 = \sigma(c_2), \ldots, c_j = \sigma(c_{j-1}).$$

Let

$$a_j = c_1 + c_2 z_j + c_3 z_j^2 + \cdots + c_p z_j^{p-1}.$$

Then, using the fact that $z_j^p = 1$,

$$\sigma(a_j) = c_2 + c_3 z_j + \cdots + c_p z_j^{p-2} + c_1 z_j^{p-1} = \frac{a_j}{z_j}.$$

So $\sigma(a_j^p) = (\sigma(a_j))^p = \frac{a_j^p}{z_j^p} = a_j^p$. Thus, $g(a_j^p) = a_j^p \ \forall g \in G$, ie. $a_j^p \in F$. Letting

$$M = \begin{pmatrix} 1 & z_1 & z_1^2 & \cdots & z_1^{p-1} \\ 1 & z_2 & z_2^2 & \cdots & z_2^{p-1} \\ & & \vdots & & \\ 1 & z_p & z_p^2 & \cdots & z_p^{p-1} \end{pmatrix},$$

we have

$$M \begin{pmatrix} c_1 \\ \vdots \\ c_p \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_p \end{pmatrix}.$$

Since M has entries in F and

$$\det M = \prod_{i<j} (z_i - z_j) \neq 0,$$

we can write $c = c_1$ as an F-linear combination of $a_1, \ldots, a_p$. Since $c \notin F$, not all a_j are in F.

Let $u = a_j$ s.t. $a_j \notin F$. Then $E = F(u)$ (by the same reasoning that showed $E = F(c)$) and $u^p = a_j^p \in F$. □

Theorem 3.12.4. *Let $p(x) \in F[x]$ be solvable by radicals over F, where* $\operatorname{char} F = 0$. *Then $\exists$ a sequence of field extensions*

$$F = L_0 \subset L_1 \subset \cdots \subset L_k = L$$

where $L_\lambda = L_{\lambda-1}(\alpha_\lambda)$, s.t. $\alpha_\lambda^{s_\lambda} \in L_{\lambda-1}$ for some s_λ and L is normal over F and contains the splitting field of $p(x)$.

Proof. By definition, $\exists$ a sequence

$$F = K_0 \subset K_1 \subset \cdots \subset K_m = K$$

where $K_j = K_{j-1}(w_j)$ with $w_j^{r_j} \in K_{j-1}$ for some r_j, and $p(x)$ splits in K.

Write $K = F(a)$ and let L be the splitting field of the min. poly. of a over F. Thus L is normal over F. Let

$$G = G(L, F) = \{\sigma_0, \ldots, \sigma_{t-1}\}, \quad \text{where } |G| = t.$$

Since $K = F(w_1, w_2, \ldots, w_m)$,

$$L = F(\sigma_0 w_1, \sigma_1 w_1, \ldots, \sigma_{t-1} w_1, \sigma_0 w_2, \ldots, \sigma_{t-1} w_2, \ldots, \sigma_0 w_m, \ldots, \sigma_{t-1} w_m).$$

Label these generators α_λ, ie. let $\alpha_\lambda = \sigma_i w_{j+1}$ where

$$\lambda - 1 = i + tj, \quad 0 \leq i \leq t-1, \quad 0 \leq j \leq m-1.$$

Inductively define $L_0 := F, L_\lambda = L_{\lambda-1}(\alpha_\lambda)$ for $1 \leq \lambda \leq tm$.

Given λ, write $\lambda - 1 = i + tj$ where $0 \leq i \leq t-1, 0 \leq j \leq m-1$. Then

$$\alpha_\lambda^{r_{j+1}} = (\sigma_i w_{j+1})^{r_{j+1}} = \sigma_i \left(w_{j+1}^{r_{j+1}} \right) \in \sigma_i(K_j) = F(\sigma_i w_1, \ldots, \sigma_i w_j) \subset L_{\lambda-1}.$$

Thus, setting $s_\lambda = r_{j+1}$ satisfies the statement of the theorem. □

Theorem 3.12.5. *Let F be a field with* $\operatorname{char} F = 0$ *and let $f(x) \in F[x]$. Then $f(x)$ is solvable by radicals $\iff$ the Galois group of $f(x)$ over F is a solvable group.*

Proof.

$\Rightarrow$: Suppose $f(x)$ is solvable by radicals. Then $\exists$ a sequence of field extensions

$$F = L_0 \subset L_1 \subset \cdots \subset L_k = L$$

where $L_j = L_{j-1}(\alpha_j)$, s.t. $\alpha_j^{r_j} \in L_{j-1}$ and L is normal over F and $f(x)$ splits in L. Since L is normal, L is the splitting field of some $g(x) \in F[x]$. Let $n = \operatorname{lcm}\{r_1, \ldots, r_j\}$ and let

$$w = e^{\frac{2\pi i}{n}}.$$

Let $G = G(L, F)$ and $H = G(L(w), F)$. L is normal over F, so by the Fund. Thm. (part 5),

$$G \cong H / G(L(w), L).$$

$G(L(w), L)$ is abelian, so to show G is solvable, it suffices to show that H is solvable.

Let

$$H_0 = G(L(w), F)$$

and for $i \geq 1$,

$$H_i = G(L(w), L_{i-1}(w)).$$

Then $H_0 = H$ and $H_{k+1} = \{e\}$. $F(w)$ is normal over F, and by Theorem 3.12.2, $L_i(w)$ is normal over $L_{i-1}(w)$ for each i. So by the Fund. Thm. (parts 4 and 5), $H_{i+1} \lhd H_i$ and

$$H_i / H_{i+1} \cong G(L_i(w), L_{i-1}(w)),$$

for $i \geq 1$, whereas

$$H_0/H_1 \cong G(F(w), F).$$

By Theorem 3.12.2, $G(L_i(w), L_{i-1}(w))$ is cyclic and thus abelian. $G(F(w), F)$ is also abelian. Hence, H is solvable, and so G is solvable.

$\Leftarrow$: Suppose that the Galois group of $f(x)$ over F is a solvable group. Let E be the splitting field of $f(x)$ over F. Let $G = G(E, F)$ and let $n = |G|$. Let $F_0 = F$ and $F_1 = F_0(w)$ where $w = e^{\frac{2\pi i}{n}}$. Let $K = E(w)$. By the Fund. Thm. (part 5),

$$G(K, F)/G \cong G(E(w), E),$$

which is abelian, so $G(K, F)$ is solvable. By Theorem 3.10.9, $G(K, F_1)$ is isomorphic to a subgroup H of $G(K, F)$, so it too is solvable.

So $\exists$ subgroups

$$\{e\} = H_{r+1} \lhd H_r \lhd \cdots \lhd H_2 \lhd H_1 = H$$

s.t. H_j/H_{j+1} is cyclic of prime order.

By the Fund. Thm., corresponding to this is a sequence of fields

$$F_1 \subset F_2 \subset \cdots \subset F_{r+1}$$

where $F_j = K^{H_j}$, so that $H_j = G(K, F_j)$. F_j is normal over F_{j+1} with cyclic Galois group of prime order p_j. Since $p_j \mid |G| = n$ and $e^{\frac{2\pi i}{n}} \in F_j$, F_j contains all the p_j^{th} roots of 1. By Theorem 3.12.3, this implies that

$$F_{j+1} = F_j(\alpha_j)$$

where $\alpha_j^{p_j} \in F_j$. Since $F_{r+1} = K$ contains the splitting field of $f(x)$, $f(x)$ is solvable by radicals over F.

□

Theorem 3.12.6. *The Galois group of $p(x) = x^n + a_1x^{n+1} + \cdots + a_{n-1}x + a_n$ over $K(a_1, \ldots, a_n)[x]$ is S_n.*

Proof. Let $r_1, \ldots, r_n$ be the roots of $p(x)$ in some extension field M of $K(a_1, \ldots, a_n)$. Then the splitting field of $p(x)$ is $K(r_1, \ldots, r_n)$, and

$$a_j = \pm s_j(r_1, \ldots, r_n) \quad \text{(the } j^{\text{th}} \text{ symmetric poly.)}.$$

$\therefore$ The Galois group of $p(x)$ is S_n by Theorem 3.9.2. □

Corollary 3.12.7. *The general n^{th} order polynomial is not solvable by radicals if $n \geq 5$.*

3.13 Calculation of Galois Groups: Cubics and Quartics

Let $f(x) \in F[x]$. Let E be the splitting field of $f(x)$ over F. Suppose E is separable over F. Let $G = G(E, F)$ be the Galois group of $f(x)$ over F and let $\alpha_1, \ldots, \alpha_n \in E$ be the roots of $f(x)$.

As noted earlier, each $\sigma \in G$ permutes $\alpha_1, \ldots, \alpha_n$, and this association yields a homo.

$$G \subset S_n.$$

What properties must this subgroup have?

Definition 3.13.1. *A subgroup $G \subset S_n$ is called **transitive** if $\forall i, j \; \exists \sigma \in G$ s.t. $\sigma(i) = j$.*

Example 3.13.2. *$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\} \subset S_4$ is transitive.*
$\{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \subset S_4$ is not transitive.

If $k < n$ then $S_k \subset S_n$ cannot be transitive. So, to have a chance for G to be transitive in $S_{\deg f(x)}$, $f(x)$ must have distinct roots.

Theorem 3.13.3. *Let $n = \deg f(x)$. Then $G \subset S_n$ is transitive $\iff$ $f(x)$ is irreducible in $F[x]$.*

Proof.

$\Leftarrow$: Suppose $f(x)$ is irreducible. Then by Theorem 3.3.15, for any pair of roots α, β of $f(x)$, $\exists \sigma \in G$ s.t. $\sigma(\alpha) = \beta$. So G is transitive.

$\Rightarrow$: Suppose G is transitive. If $f(x)$ is reducible, write

$$f(x) = g(x)h(x)$$

where $g(x)$ is irreducible. Let α be a root of $g(x)$. If β is any root of $f(x)$, then find $\sigma \in G$ s.t. $\sigma(\alpha) = \beta$. Since $g \in F[x]$ and σ fixes F, this means that β is also a root of $g(x)$. This shows that every root of $f(x)$ is a root of $g(x)$. But G transitive $\Rightarrow$ the roots of $f(x)$ are distinct, so roots of $h(x)$ are not roots of $g(x)$, which is a contradiction. Hence $f(x)$ is irreducible.

□

Let $h(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$. Let

$$H = \{\sigma \in S_n \mid \sigma h = h\}$$

where σ acts by permuting the variables, ie.

$$h \cdot \sigma = (\sigma^{-1}h)(y_1, \ldots, y_n) := h(y_{\sigma(1)}, \ldots, y_{\sigma(n)}).$$

$H \leq S_n$ is called the **isotropy subgroup** of h.

Example 3.13.4. *$n = 4$, $h = y_1 + y_2$. Then $H = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.*

Let $\delta = h(\alpha_1, \ldots, \alpha_n) \in E$. If $\sigma \in G \cap H$ then $\sigma(\delta) = \delta$, so

$$\sigma \in G(E, F(\delta)).$$

When is $G(E, F(\delta)) = G \cap H$?

Example 3.13.5.

1. *$n = 3$,*

   $$h(y_1, y_2, y_3) = (y_1 - y_2)(y_1 - y_3)(y_2 - y_3).$$

   Then $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} = A_3$. Let $f(x)$ be an irreducible cubic over F with roots $\alpha_1, \alpha_2, \alpha_3$. Assume $\operatorname{char} F \neq 2$. *Let*

   $$\Delta = h(\alpha_1, \alpha_2, \alpha_3).$$

   For $\sigma \in G$, if $\sigma \in H$ then $\sigma(\Delta) = \Delta$. If $\sigma \notin H$ then $\sigma(\Delta) = -\Delta \neq \Delta$. So

   $$\sigma(\Delta) = \Delta \iff \sigma \in G \cap H.$$

   $\therefore G \cap H = G(E, F(\Delta))$.

2. *$n = 4, h = y_1 + y_4$. Let $f(x) = x^4 - x^2 + 1$ over $F = \mathbb{Q}$. Then*

   $$H = \{e, (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}.$$

   Also,

   $$f(x) = x^4 - x^2 + 1 = (x^2+1)^2 - 3x^2 = (x^2 + 1 + \sqrt{3}x)(x^2 + 1 - \sqrt{3}x) = (x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1).$$

   So the roots are

   $$\frac{-\sqrt{3} \pm \sqrt{3-4}}{2}, \quad \frac{\sqrt{3} \pm \sqrt{3-4}}{2}.$$

   Let

   $$\alpha_1 = \frac{-\sqrt{3} + i}{2},\ \alpha_2 = \frac{-\sqrt{3} - i}{2},\ \alpha_3 = \frac{\sqrt{3} + i}{2},\ \alpha_4 = \frac{\sqrt{3} - i}{2},$$

   and with this numbering of the roots, $H \subset G$. So

   $$\delta = h(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha_1 + \alpha_4 = 0.$$

   Consider complex conjugation σ. $\sigma \in G$ and acts on the roots as $\sigma = (1\ 2)(3\ 4)$, so $\sigma \notin H$. But $\sigma(0) = 0$. So in this case,

   $$H = G \cap H \subsetneq G(E, F(\delta)) = G(E, F(0)) = G(E, F).$$

More generally, suppose

$$\delta_j = h_j(\alpha_1, \ldots, \alpha_n) \in E$$

for $j = 1, \ldots, k$, where $h_j \in F[y_1, \ldots, y_n]$. Define the isotropy subgroup by

$$H = \{\sigma \in S_n \mid \sigma h_j = h_j \ \forall j = 1, \ldots, k\}.$$

In general:

Theorem 3.13.6. *Let*

$$\delta_j = h_j(\alpha_1, \ldots, \alpha_n) \in E$$

where $h_j(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$. Let $H \subset S_n$ be the isotropy subgroup of $\{h_j\}$. Suppose that for all $\sigma \in G - H$, $\exists j$ s.t. $\sigma(\delta_j) \neq \delta_j$. Then

$$G(E, F(\delta_1, \ldots, \delta_n)) = G \cap H.$$

Proof. $G \cap H \subset G(E, F(\delta_1, \ldots, \delta_n))$ in general. Suppose $\sigma \in G(E, F(\delta_1, \ldots, \delta_n)) \subset G(E, F) = G$. Then $\sigma(\delta_j) = \delta_j \ \forall j$ so $\sigma \in H$, since if $\sigma \notin H$ then $\exists j$ s.t. $\sigma(\delta_j) \neq \delta_j$. □

Note: It is often not so easy to check whether or not the condition $\sigma(\delta) \neq \delta \ \forall \sigma \in G - H$ is satisfied.

3.14 Cubics

3.14.1 Galois Theory of Cubics

Let

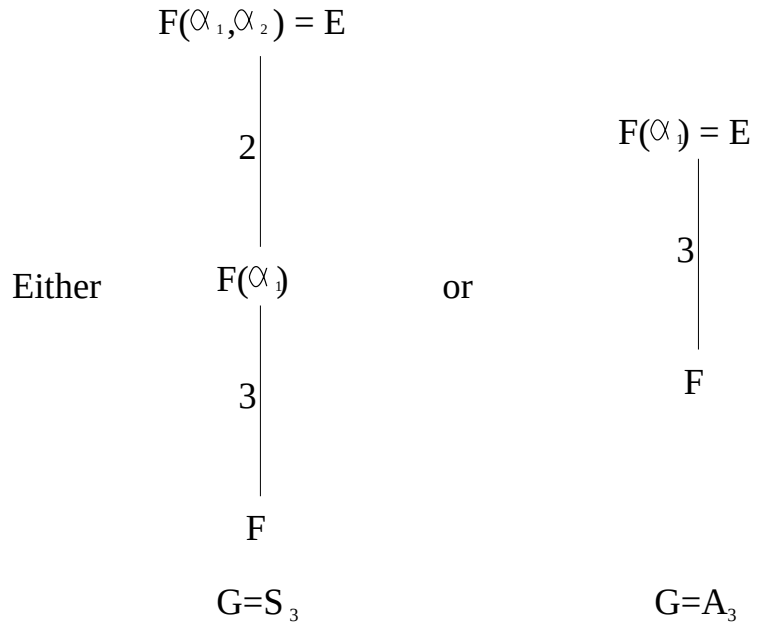
$$k(z) = z^3 + az^2 + bz + c$$

be irreducible, $a, b, c \in F$. Assume $\operatorname{char} F \neq 2, 3$. Let $z = x - \frac{a}{3}$ to get

$$f(x) = x^3 + px + q$$

where $p = \frac{3b - a^2}{3}, q = \frac{2a^3 - 9ab + 27c}{27}$. This adds $\frac{a}{3}$ to each root, but does not affect the Galois group since $\frac{a}{3} \in F$.

Let E be the splitting field of f and let $G = G(E, F)$ be the Galois group of f. Since $G \subset S_3$, and G is transitive, there are only 2 possibilities: $G = S_3$ or $G = A_3$.



ie. Depending on a, b, c, either $F(\alpha_1)$ already contains α_2 and α_3 so that $E = F(\alpha_1)$ and $G = A_3$ or it does not and we have a further degree 2 extension. How do we tell which?

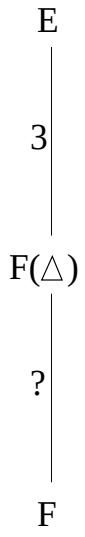
Let

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

$f(x)$ is irreducible and char $F \neq 3 \Rightarrow$ the roots are distinct $\Rightarrow \Delta \neq 0$.

$$H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} = A_3 \subset G.$$

If $\sigma \notin H$ then $\sigma(\Delta) = -\Delta \neq \Delta$.. The theorem implies $G(E, F(\Delta)) = G \cap H = A_3$. So in either case we have:



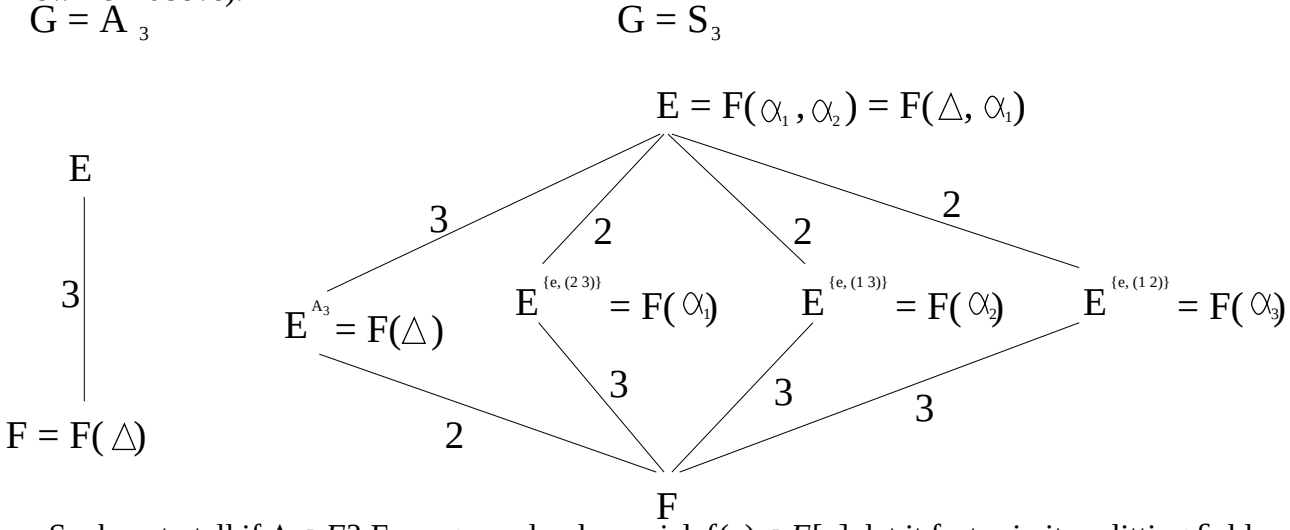
If $\Delta \in F$ then $F(\Delta) = F$ so

$$G(E, F) = G(E, F(\Delta)) = A_3.$$

If $\Delta \notin F$ then $[F(\Delta) : F] > 1$ so $[E : F] > 3$, so $G = S_3$.
Note: $\sigma(\Delta) = \pm\Delta \ \forall \sigma \in G$ so

$$\sigma(\Delta^2) = \Delta^2 \ \forall \sigma \in G.$$

$\therefore \Delta^2 \in F$ in any case. (This also shows that if $\Delta \notin F$ then $[F(\Delta) : F] = 2$, confirming what we already know from above).



So, how to tell if $\Delta \in F$? For a general polynomial $f(x) \in F[x]$, let it factor in its splitting field as

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i).$$

Let

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j).$$

The sign of Δ depends on our choice of the order of the roots. Set $D = \Delta^2$. Then D is fixed by all permutations of $\{\alpha_j\}$, (since for each permutation σ, $\sigma(\Delta) = \pm\Delta$). So $D \in F$. D is called the **discriminant** of $f(x)$.

$n = 2$: $f(x) = x^2 + bx + c$;

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4c}}{2}, \quad \alpha_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

$\therefore \Delta = \alpha_1 - \alpha_2 = \sqrt{b^2 - 4c}$ and $D = b^2 - 4c$.

$n = 3$: $f(x) = x^3 + ax^2 + bx + c$. As before, let $x = y - \frac{a}{3}$ to get

$$g(y) = y^3 + py + q$$

where $p = \frac{1}{3}(3b - a^2)$ and $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

$$g(y) = (y - \alpha)(y - \beta)(y - \gamma)$$

in an extension field.

$$\begin{aligned} s_1 &= \alpha + \beta + \gamma = 0, \\ s_2 &= \alpha\beta + \beta\gamma + \alpha\gamma = p, \\ s_3 &= \alpha\beta\gamma = -q. \end{aligned}$$

Then

$$\begin{aligned} 3y^2 + p &= g'(y) \\ &= (y - \alpha)(y - \beta) + (y - \alpha)(y - \gamma) + (y - \beta)(y - \gamma) \\ \therefore \quad g'(\alpha) &= (\alpha - \beta)(\alpha - \gamma) \\ g'(\beta) &= (\beta - \alpha)(\beta - \gamma) \\ g'(\gamma) &= (\gamma - \alpha)(\gamma - \beta) \end{aligned}$$

$$\therefore \quad D = -g'(\alpha)g'(\beta)g'(\gamma).$$

That is,

$$\begin{aligned} D &= -(3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) \\ &= -27\alpha^2\beta^2\gamma^2 - 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) - 3p^2(\alpha^2 + \beta^2 + \gamma^2) - p^3 \\ &= -27s_3^2 - 9p(s_2^2 - 2s_1s_3) - 3p^2(s_1^2 - 2s_2) - p^3 \\ &= -27q^2 - 9p(p^2 - 0) - 3p^2(-2p) - p^3 \\ &= -4p^3 - 27q^2 \\ &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2. \end{aligned}$$

3.14.2 Solution of Cubics

$$0 = x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

That is,

$$\begin{aligned}\alpha_1 + \alpha_2 + \alpha_3 &= 0\\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= p\\ \alpha_1\alpha_2\alpha_3 &= -q\end{aligned}$$

Find $\alpha_1, \alpha_2, \alpha_3$.

Let

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \sqrt{-4p^3 - 27q^2}.$$

Let $\omega = e^{\frac{2\pi i}{3}}$ so that $\omega^3 = e^{2\pi i} = 1$, ie. ω satisfies

$$0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1).$$

Explicitly,

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

Let

$$\begin{aligned}z_1 &= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3\\ z_2 &= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\\ z_3 &= \alpha_1 + \alpha_2 + \alpha_3 = 0\end{aligned}$$

ie.

$$\begin{pmatrix} z_1 \\ z_2 \\ 0 \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \quad \text{where } A = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \\ 1 & 1 & 1 \end{pmatrix}.$$

If we can find z_1, z_2 then $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = A^{-1} \begin{pmatrix} z_1 \\ z_2 \\ 0 \end{pmatrix}$. Explicitly,

$$\begin{aligned}\alpha_1 &= \frac{1}{3}(z_1 + z_2)\\ \alpha_2 &= \frac{1}{3}(\omega^2 z_1 + \omega z_2)\\ \alpha_3 &= \frac{1}{3}(\omega z_1 + \omega^2 z_2).\end{aligned}$$

To find z_1, z_2:

$$\begin{aligned} z_1^3 =& \alpha_1^3 + \omega^3\alpha_2^3 + \omega^6\alpha_3^3 + 3\omega\alpha_1\alpha_2 + 3\alpha_1\omega^2\alpha_2^2 \\ &+ 3\omega^2\alpha_1^2\alpha_3 + 3\omega^4\alpha_1\alpha_3^2 + 3\omega^4\alpha_2^2\alpha_3 + 3\omega^5\alpha_2\alpha_3^2 + 6\omega^3\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Using the facts that $\alpha_j^3 = -p\alpha_j - q$, $\omega^3 = 1$, and $\omega^2 = -\omega - 1$, this becomes

$$\begin{aligned} z_1^3 &= -p\alpha_1 - q - p\alpha_2 - q - p\alpha_3 - q \\ &\quad + 3\omega(\alpha_1^2\alpha_2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_3^2) + 6\alpha_1\alpha_2\alpha_3 \\ &= -p(\alpha_1 + \alpha_2 + \alpha_3) - 3q - 3\omega(\alpha_1^2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_3^2) - 6q \\ &= -9q + 3\omega u + 3\omega^2 v \end{aligned}$$

where

$$\begin{aligned} u &= \alpha_1^2\alpha_2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3 \quad \text{and} \\ v &= \alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_3^2. \end{aligned}$$

Now,

$$\begin{aligned} 0 &= (\alpha_1 + \alpha_2 + \alpha_3)^3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\alpha_1^2\alpha_2 + 3\alpha_1^2\alpha_3 + 3\alpha_2^2\alpha_3 + 3\alpha_1\alpha_2^2 + 3\alpha_1\alpha_3^2 + 3\alpha_2\alpha_3^2 + 6\alpha_1\alpha_2\alpha_3 \\ &= -p\alpha_1 - q - p\alpha_2 - q - p\alpha_3 - q + 3u + 3v - 6q \\ &= -9q + 3u + 3v. \end{aligned}$$

$\therefore u + v = 3q$. Also,

$$\begin{aligned} \Delta &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\ &= \alpha_1^2\alpha_2 - \alpha_1^2\alpha_3 - \alpha_1\alpha_2^2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3 - \alpha_2\alpha_3^2 \\ &= u - v. \end{aligned}$$

Using the equations $u + v = 3q$ and $u - v = \Delta$, get

$$\begin{aligned} u &= \frac{3}{2}q + \frac{\Delta}{2} \\ v &= \frac{3}{2}q - \frac{\Delta}{2}. \end{aligned}$$

So

$$\begin{aligned} z_1^3 &= -9q + 3\omega u + 3\omega^2 v \\ &= -9q + \omega\frac{9}{2}q + \omega\frac{3}{2}\Delta + \omega^2\frac{9}{2}q - \omega^2\frac{3}{2}\Delta \\ &= -9q + \omega\frac{9}{2}q + \omega\frac{3}{2}\Delta - \omega\frac{9}{2}q - \frac{9}{2}q - \omega\frac{3}{2}\Delta + \frac{3}{2}\Delta \\ &= -\frac{27q}{2} + 3\omega\Delta + \frac{3}{2}\Delta \\ &= -\frac{27q}{2} + \frac{3}{2}\Delta(2\omega + 1) \\ &= -\frac{27q}{2} + \frac{3\sqrt{3}i}{2}\Delta. \end{aligned}$$

Similarly, we find

$$z_2^3 = \overline{z_1}^3 = -\frac{27q}{2} - \frac{3\sqrt{3}i}{2}\Delta.$$

$\therefore z_1 = (-\frac{27q}{2} + \frac{3\sqrt{3}i}{2}\Delta)^{\frac{1}{3}}$ and $z_2 = (-\frac{27q}{2} - \frac{3\sqrt{3}i}{2}\Delta)^{\frac{1}{3}}$. This determines $\alpha_1, \alpha_2, \alpha_3$ in terms of p and q.

To illustrate the Galois theory, we now find a formula for α_2 in terms of α_1, that makes is obvious that $\alpha_2 \in F(\alpha_1) \iff \Delta \in F$.

$$\begin{aligned} \Delta &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\ &= (\alpha_1 - \alpha_2)(2\alpha_1 + \alpha_2)(\alpha_1 + 2\alpha_2), \quad \text{since } \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ &= 2\alpha_1^3 + 5\alpha_1^2\alpha_2 + 2\alpha_1\alpha_2^2 - 2\alpha_1^2\alpha_2 - 5\alpha_1\alpha_2^2 - 2\alpha_2^3 \\ &= -2\alpha_1 p - 2q + 3\alpha_1^2\alpha_2 - 3\alpha_1\alpha_2^2 + 2\alpha_2 p + 2q \\ &= -2\alpha_1 p + 3\alpha_1^2\alpha_2 - 3\alpha_1\alpha_2^2 + 2\alpha_2 p. \end{aligned}$$

Also,

$$q = -\alpha_1\alpha_2\alpha_3 = \alpha_1\alpha_2(\alpha_1 + \alpha_2) = \alpha_1^2\alpha_2 + \alpha_1\alpha_2^2 \Rightarrow \alpha_1\alpha_2^2 = q - \alpha_1^2\alpha_2.$$

So,

$$\begin{aligned} \Delta &= -2\alpha_1 p + 3\alpha_1^2\alpha_2 - 3q + 3\alpha_1^2\alpha_2 + 2\alpha_2 p \\ &= -2\alpha_1 p + 6\alpha_1^2\alpha_2 - 3q + 2\alpha_2 p. \end{aligned}$$

$\therefore 6\alpha_1^2\alpha_2 + 2\alpha_2 p = \Delta + 2\alpha_1 p + 3q$. This gives

$$\alpha_2 = \frac{\Delta + 2\alpha_1 p + 3q}{2(3\alpha_1^2 + p)}. \qquad (*)$$

Thus, if $\Delta \in F$ then $\alpha_2 \in F(\alpha_1)$. Conversely, if $\alpha_2 \in F(\alpha_1)$ then (*) $\Rightarrow \Delta \in F(\alpha_1)$. But

$$[F(\alpha_1) : F] = 3$$

and $\Delta^2 \in F$, so this implies that $\Delta \in F$.

3.15 Quartics

3.15.1 Solution of Quartics

We want to solve

$$z^4 + a_1 z^3 + a_2 z^2 + a_3 z + a_4 = 0.$$

Let $z = x - \frac{a}{4}$ to get the form

$$x^4 + px^2 + qx + r = 0.$$

Let the roots be r_1, r_2, r_3, r_4, so

$$\begin{aligned} s_1 &= r_1 + r_2 + r_3 + r_4 = 0 \\ s_2 &= r_1 r_2 + r_1 r_3 + r_1 r_4 + r_2 r_3 + r_2 r_4 + r_3 r_4 = p \\ s_3 &= r_1 r_2 r_3 + r_1 r_2 r_4 + r_1 r_3 r_4 + r_2 r_3 r_4 = -q \\ s_4 &= r_1 r_2 r_3 r_4 = r. \end{aligned}$$

Suppose we can determine

$$\begin{aligned} (r_1 + r_2)(r_3 + r_4) &= \theta_1 \\ (r_1 + r_3)(r_2 + r_4) &= \theta_2 \\ (r_1 + r_4)(r_2 + r_3) &= \theta_3. \end{aligned}$$

Then letting $a = r_1 + r_2, b = r_3 + r_4$, get $ab = \theta_1$ and $a + b = 0$. So $-a^2 = ab = \theta_1$, so

$$a = \sqrt{-\theta_1}, \quad b = -\sqrt{-\theta_1},$$

where $\sqrt{-\theta_1}$ is one of the square roots of $-\theta_1$ in $\mathbb{C}$.

Similarly,

$$\begin{aligned} r_1 + r_3 &= \sqrt{-\theta_2}, \quad r_2 + r_4 = -\sqrt{-\theta_2}, \\ r_1 + r_4 &= \sqrt{-\theta_3}, \quad r_2 + r_3 = -\sqrt{-\theta_3}, \end{aligned}$$

for choices of $\sqrt{-\theta_2},\ \sqrt{-\theta_3}$. So

$$\begin{aligned}\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3} &= r_1+r_2+r_1+r_3+r_1+r_4\\ &= 2r_1+r_1+r_2+r_3+r_4\\ &= 2r_1.\\ \therefore\ r_1 &= \frac{\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3}}{2}.\end{aligned}$$

Similarly, we can solve for r_2, r_3, r_4 if we know $\theta_1, \theta_2, \theta_3$. So it suffices to find $\theta_1, \theta_2, \theta_3$.

Consider the cubic equation

$$f(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3) = 0.$$

If we can write the coefficients of this eqn. in terms of p, q, r, then we can use the soln. of cubics to determine $\theta_1, \theta_2, \theta_3$ in terms of p, q, r and thus write r_1, r_2, r_3, r_4 in terms of p, q, r.

Consider the action of S_4 as permutations of r_1, r_2, r_3, r_4. Consider first the transposition σ which interchanges r_1 and r_2:

$$\sigma(\theta_1) = \theta_1 \quad \sigma(\theta_2) = \theta_3 \quad \sigma(\theta_3) = \theta_2.$$

$\therefore \sigma(f(x)) = f(x)$.

Similarly, $\sigma(f(x)) = f(x)$ for every transposition in S_4. Since S_4 is generated by transpositions, $\sigma(f(x)) = f(x)\ \forall \sigma \in S_4$. That is, the coeffs. of $f(x)$ are left fixed by all permutations of r_1, r_2, r_3, r_4. So the coeffs. of $f(x)$ are symmetric polynomials in r_1, r_2, r_3, r_4, and so can be expressed in terms of p, q, r. This gives:

Theorem 3.15.1. *The coefficients of $f(x)$ are polynomials in p, q, r.*

To find the coefficients:

Method 1: Expand

$$\begin{aligned}f(x) &= (x-(r_1+r_2)(r_3+r_4))(x-(r_1+r_3)(r_2+r_4))(x-(r_1+r_4)(r_2+r_3))\\ &= \text{big mess}\\ &= \text{poly. in } p, q, r, x.\end{aligned}$$

Or

Method 2: Geometric method using conics.

3.15.2 Conics (over $\mathbb{R}$)

Definition 3.15.2. *A **conic** is a polynomial of degree ≤ 2 in two variables (over $\mathbb{R}$),*

$$q(x,y) = ax^2 + bxy + cy^2 + dx + ey + f.$$

To conic $q(x,y)$, associate the 3-variable quadratic form:

$$Q(X,Y,Z) = aX^2 + bXY + cY^2 + dXZ + cYZ + fZ^2.$$

ie. $Q(X,Y,Z) = Z^2 q(\frac{X}{Z}, \frac{Y}{Z})$. The **associated matrix** to q is

$$M_q = \begin{pmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{pmatrix},$$

and this gives

$$Q(X,Y,Z) = \begin{pmatrix} X & Y & Z \end{pmatrix} M_q \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

M_q is symmetric, so it is diagonalizable. ie. $\exists U$ s.t.

$$U^{-1} M_q U = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}.$$

This corresponds to change of variables

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = U \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix}.$$

In the new basis,

$$Q'(X',Y',Z') = \lambda_1 X'^2 + \lambda_2 Y'^2 + \lambda_3 Z'^2.$$

$\det M_q = \lambda_1\lambda_2\lambda_3$. If $\det M_q = 0$ then $Q = 0$ degenerates into a product of lines.

e.g. Suppose $\lambda_3 = 0$. If λ_1, λ_2 have the same sign then $Q' = 0 \iff X' = 0, Y' = 0$, giving one line. If λ_1, λ_2 have different signs then

$$0 = Q' = \lambda_1 X'^2 + \lambda_2 Y'^2$$

factors into linear factors, giving two planes. So $q(x,y)$ degenerates when $\det M_q = 0$.

Conversely, if $q(x, y)$ factors as a product

$$q(x, y) = (\alpha x + \beta y + \gamma)(\delta x + \epsilon y + \varphi)$$

then Q factors as

$$(\alpha X + \beta Y + \gamma Z)(\delta X + \epsilon Y + \varphi Z),$$

and by inspection, this can only happen when one of the λ_i's is 0. So $q(x, y)$ is degenerate $\iff$ $\det M_q = 0$.

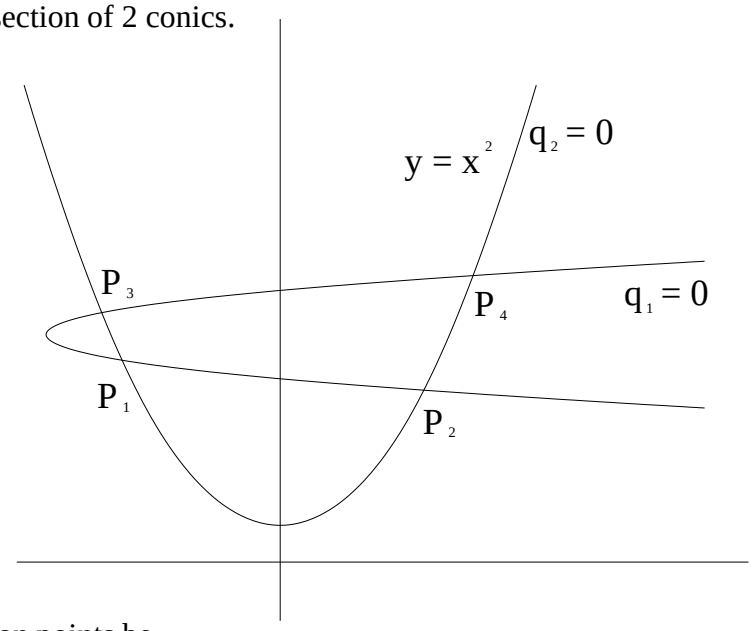
Consider the quartic

$$x^4 + px^2 + qx + r = 0.$$

Let $y = x^2$. Then solving $x^4 + px^2 + qx + r = 0$ is equivalent to solving the system

$$q_1 = y^2 + py + qx + r = 0,$$
$$q_2 = y - x^2 = 0.$$

$\therefore$ Look for the intersection of 2 conics.



Let the intersection points be

$$P_1 = (r_1, r_1^2), \quad P_2 = (r_2, r_2^2), \quad P_3 = (r_3, r_3^2), \quad P_4 = (r_4, r_4^2).$$

Consider the family of conics $q_t = q_1 - tq_2$. Then $q_t(P_j) = 0$ regardless of t. Since M_{q_t} is a 3×3 matrix, $\det M_{q_t} = 0$ is a cubic eqn. in t. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $\det M_{q_t}$. We will show that $\alpha_1, \alpha_2, \alpha_3$ are $\theta_1, \theta_2, \theta_3$.

For $j = 1, 2, 3$, $\det M_{q_{\alpha_j}} = 0$, so q_{α_j} is a product of lines. We know that P_1, P_2, P_3, P_4 satisfy $q_t = 0\ \forall t$ so they must lie on the lines. So the lines have to be those joining the points P_j. Let $L_{ij} = 0$ be the line joining P_i to P_j. Then (upon renumbering if necessary),

$$q_{\alpha_1} = L_{12}L_{34}, \quad q_{\alpha_2} = L_{13}L_{24}, \quad q_{\alpha_3} = L_{14}L_{23}.$$

L_{12} is

$$y - r_1^2 = \left(\frac{r_2^2 - r_1^2}{r_2 - r_1}\right)(x - r_1) = (r_2 + r_1)(x - r_1) = (r_1 + r_2)x - r_1r_2 - r_1^2$$

That is, L_{12} is $y - (r_1 + r_2)x + r_1r_2 = 0$. Similarly, L_{34} is $y - (r_3 + r_4)x + r_3r_4 = 0$.

To show $\alpha_1 = \theta_1$:

$$\begin{aligned}
q_1 - \alpha_1 q_2 = q_{\alpha_1} &= (y - (r_1 + r_2)x + r_1r_2)(y - (r_3 + r_4)x + r_3r_4) \\
&= y^2 - (r_1 + r_2 + r_3 + r_4)xy + (r_1 + r_2)(r_3 + r_4)x^2 - (r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4)x \\
&\quad + (r_1r_2 + r_3r_4)y + r_1r_2r_3r_4 \\
&= y^2 + \theta_1 x^2 + qx + (p - r_1r_3 - r_1r_4 - r_2r_3 - r_2r_4)y + r \\
&= y^2 + \theta_1 x^2 + qx + py - (r_1 + r_2)(r_3 + r_4)y + r \\
&= y^2 + \theta_1 x^2 + qx + py - \theta_1 y + r \\
&= q_1 - \theta_1 q_2.
\end{aligned}$$

$\therefore \alpha_1 = \theta_1$. Similarly, $\alpha_2 = \theta_2$ and $\alpha_3 = \theta_3$. So to find $\theta_1, \theta_2, \theta_3$, we must solve $\det M_{q_t} = 0$

$$q_t = q_1 - tq_2 = y^2 + py + qx + r - t(y - x^2) = y^2 + tx^2 + qx + (p - t)y + r.$$

So

$$\begin{aligned}
\det M_{q_t} &= \begin{vmatrix} t & 0 & \frac{q}{2} \\ 0 & 1 & \frac{p-t}{2} \\ \frac{q}{2} & \frac{p-t}{2} & r \end{vmatrix} \\
&= tr - \frac{q^2}{4} - \left(\frac{p - t}{2}\right)^2 t \\
&= tr - \frac{q^2}{4} - \frac{p^2t}{4} + \frac{2pt^2}{4} - \frac{t^3}{4} \\
&= \frac{1}{4}(t^3 - 2pt^2 + (p^2 - 4r)t + q^2)
\end{aligned}$$

So $\det M_{q_t} = 0 \iff t^3 - 2pt^2 + (p^2 - 4r)t + q^2 = 0$.

Summary: To solve

$$z^4 + a_1z^3 + a_2z^2 + a_3z + a_4 = 0,$$

1. Let $z = x - \frac{a}{4}$ to get the form
$$x^4 + px^2 + qx + r = 0.$$
2. Solve the cubic
$$t^3 - 2pt^2 + (p^2 - 4r)t + q^2 = 0$$
to get $\theta_1, \theta_2, \theta_3$.
3. $r_1 = \frac{\sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}}{2}$ for some choice of square roots of $-\theta_1, -\theta_2, -\theta_3$, and similar formulae for the other roots.

Notice that

$$\begin{aligned}\theta_1 - \theta_2 &= (r_1 + r_2)(r_3 + r_4) - (r_1 + r_3)(r_2 + r_4)\\ &= r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 - r_1r_2 - r_1r_4 - r_2r_3 - r_3r_4\\ &= -(r_1 - r_4)(r_2 - r_3).\end{aligned}$$

Similarly, $\theta_1 - \theta_3 = -(r_1 - r_3)(r_2 - r_4)$ and $\theta_2 - \theta_3 = -(r_1 - r_2)(r_3 - r_4)$. So

$$D_{\text{cubic}} = \prod_{i \neq j}(\theta_i - \theta_j) = \prod_{i \neq j}(r_i - r_j) = D_{\text{original quartic}}.$$

Thus

$$\begin{aligned}D &= -4(-2p)^3q^2 + (-2p)^2(p^2 - 4r)^2 + 18(-2p)(p^2 - 4r)q^2 - 4(p^2 - 4r)^3 - 27(q^2)^2\\ &= 32p^3q^2 + 4p^4 - 32p^4r + 64p^2r^2 - 36p^3q^2 + 144pq^2r - 4p^6 + 48p^4r - 192p^2r^2 + 256r^3 - 27q^4\\ &= 16p^4r - 4p^3q^2 - 128p^2r + 144pq^2r - 27q^4 + 256r^3\\ &= -128b^2d^2 - 4a^3g^3 + 16x^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 + 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d\\ &\quad - 6a^2c^2d + 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd.\end{aligned}$$

3.15.3 Galois Theory of Quartics

Let
$$f(x) = x^4 + px^2 + qx + r$$
be irreducible, char $F \neq 2, 3$. Let E be the splitting field of $f(x)$ over F. Let $G = G(E, F)$ be the Galois group.

$G \subset S_4$ is transitive. The transitive subgroups of S_4 are:

1. S_4.

2. A_4.

3. The Sylow 2-subgroups, isomorphic to D_8:

$$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\},$$
$$\{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3), (1\ 2), (3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$
$$\{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2), (1\ 4), (2\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4)\}.$$

4. Groups isomorphic to C_3:

$$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}, \{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}, \{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}.$$

5. $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong C_2 \times C_2 = V$.

Let

$$g(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 - 2px^2 + (p^2 - 4r)x + q^2,$$

where

$$\theta_1 = (r_1 + r_2)(r_3 + r_4),$$
$$\theta_2 = (r_1 + r_3)(r_2 + r_4),$$
$$\theta_3 = (r_1 + r_4)(r_2 + r_3).$$

Let

$$\Delta = \prod_{i<j}(r_i - r_j) = -(\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3).$$

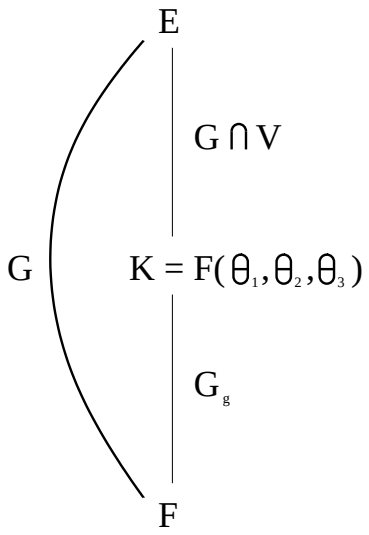
$\operatorname{char} F \neq 2$ and f irreducible $\Rightarrow$ roots are distinct, so $\Delta \neq 0$. The discriminant is

$$D = \Delta^2 \in F.$$

Let $K = F(\theta_1, \theta_2, \theta_3)$ be the splitting field of $g(x)$. $\theta_j \in E$ for $j = 1, 2, 3$ so $K \subset E$. Notice that $V \cong C_2 \times C_2$ is the isotropy group of

$$\{\theta_1, \theta_2, \theta_3\}.$$

ie. If $\sigma \in V$ then $\sigma(\theta_j) = \theta_j$, but if $\sigma \in S_4 - V$ then for some j, $\sigma(\theta_j) \neq \theta_j$. According to Theorem 3.13.6, this implies $G(E, K) = G \cap V$.



By the Fund. Thm.,

$$G_g = G(K, F) \cong G/(G \cap V).$$

We can calculate G_g from the section on cubics. Will this determine G? By inspection:

	G	$G/(G \cap V)$
1	S_4	S_3
2	A_4	C_3
3	D_8	C_2
4	C_4	C_2
5	V	$\{e\}$

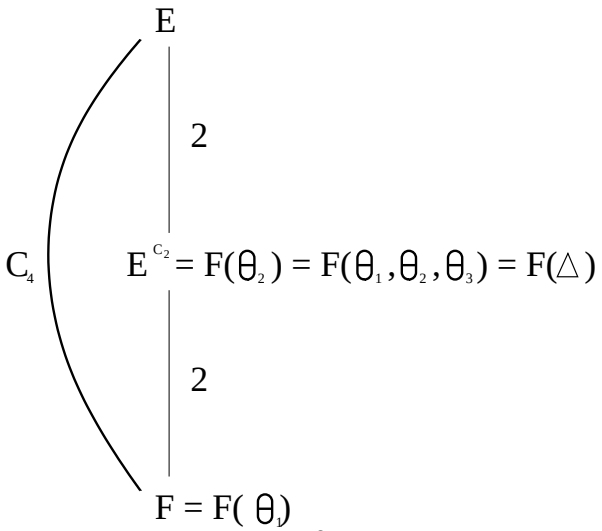
So $G_g = G/(G \cap V)$ will tell us G unless $G_g \cong C_2$, in which case it cannot distinguish between D_8 and C_4.

Study $G_g = C_2$ more closely to obtain a method of distinguishing. So assume $G_g \cong C_2$. Since $g(x)$ is a cubic and $|C_2| = 2$, this means that one root of $g(x)$, say θ_1, already lies in F. ie. In F, $g(x)$ factors as

$$g(x) = (x - \theta_1)g_1(x)$$

where $g_1(x)$ is an irreducible quadratic (with roots θ_2, θ_3, which are not in F).

Suppose $G = C_4$.



Recall $(r_1 + r_2)^2 = -\theta_1$ so $[F(r_1 + r_2) : F] \leq 2$. If $r_1 + r_2 \in F$ then $r_1 + r_2$ is fixed by all $\sigma \in G$. But $G = C_4$ contains a 4-cycle, and no 4-cycle fixes $r_1 + r_2$. e.g. Say $\sigma = (1\ 2\ 3\ 4)$. Then $\sigma(r_1 + r_2) = r_2 + r_3$.

Thus $r_1 + r_2 \notin F$, and so

$$[F(r_1 + r_2) : F] = 2.$$

C_4 has a unique subgroup of index 2, so E has a unique subfield of order 2 over F. So

$$F(r_1 + r_2) = E^{C_2} = F(\theta_2) = F(\Delta).$$

Hence $r_1 + r_2 = a + b\Delta$ for some $a, b \in F$.

$$-\theta_1^2 = (r_1 + r_2)^2 = a^2 + 2ab\Delta + b^2\Delta^2 = a^2 + b^2D + 2ab\Delta$$

where $D = \Delta^2 \in F$. So

$$2ab\Delta = -\theta_1 - a^2 - b^2D \in F.$$

But $\Delta \notin F$, so either $a = 0$ or $b = 0$. $b \neq 0$, since $b = 0$ puts $r_1 + r_2 = a \in F$, so $a = 0$. Thus

$$-\theta_1 = b^2D$$

$\therefore \frac{-\theta_1}{D}$ is a square in F.

In conclusion, $G = C_4 \Rightarrow \frac{-\theta_1}{D}$ is a square in F.

Conversely, suppose $\frac{-\theta_1}{D} = b^2$ for some $b \in F$. Then

$$(r_1 + r_2)^2 = b^2D = b^2\Delta^2$$

so $r_1 + r_2 = \pm b\Delta \in F(\Delta)$.

Suppose that $G = D_8$. Then by inspection, G contains 2 disjoint transpositions. $(1\ 2) \notin G$, since this contradicts $r_1 + r_2 = \pm b\Delta$ (any transposition applied to Δ produces $-\Delta$). So, some other transposition, say $(1\ 3)$ lies is G (since G contains 2 disjoint transpositions, one of them must include 1).

$$r_3 + r_2 = (1\ 3) \cdot (r_1 + r_2) = (1\ 3)(\pm b\Delta) = \mp b\Delta.$$

So

$$-\theta_3 = (r_3 + r_2)^2 = b^2\Delta^2 = b^2 D \in F.$$

This is a contradiction, so $G \ncong D_8$, and thus, $G \cong C_4$. ie. $G \cong C_4 \iff -\frac{\theta_1}{D}$ is a square in F.
Summary: To compute G,

1. Compute
$$g(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2.$$
2. Factor $g(x)$ in F:

Case I: $g(x)$ factors completely in F. Then $G_g = \{e\}$, so $G = V$.

Case II: $g(x)$ has one linear factor in F,

$$g(x) = (x - \theta)g_1(x).$$

(a) The factorization determines $\theta \in F$.
(b) Compute $D \in F$, the discriminant of g, by earlier formula.
(c) If $-\frac{\theta}{D}$ is a square in G, then $G = C_4$; otherwise, $G = D_8$.

Case III: $g(x)$ is irreducible over F.

(a) Compute $D \in F$ as above.
(b) If D is a square in F then $G_g = C_3 = A_3$, so $G = A_4$. Otherwise, $G_g = S_3$ so $G = S_4$.

For $G = S_4$:
$r_1 + r_2 \neq 0$, since $\theta_1 \neq 0$ (g is irreducible when $G = S_4$). Similarly, $r_i + r_j \neq 0\ \forall i, j$. So

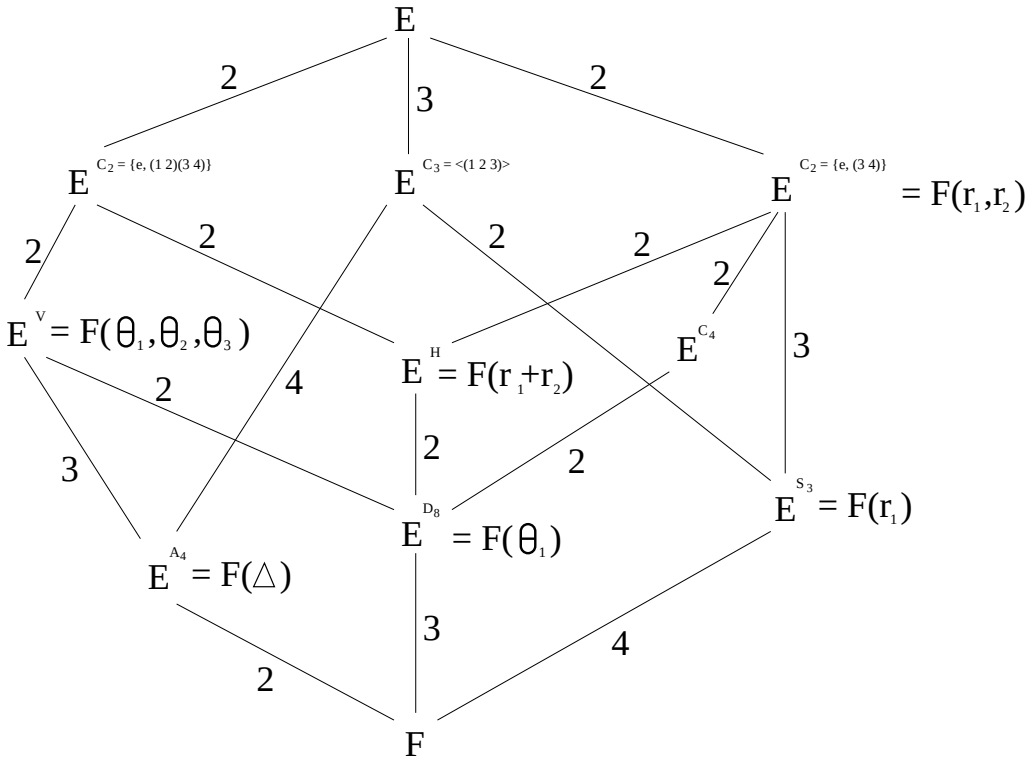
$$r_1 + r_2 \neq r_i + r_j$$

unless $i = 1, j = 2$ or $j = 1, i = 2$. Hence $\sigma(\theta_j) \neq \theta_j$ if $\sigma \in$ isotropy group of θ_1, which is D_8. Thus,

$$G(E, F(\theta_1)) \cong D_8.$$

Let

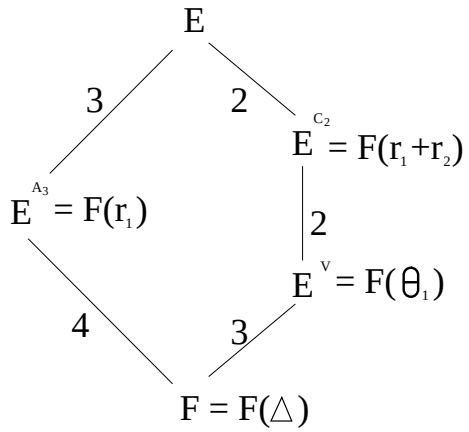
$$H = \text{isotropy group of } r_1 + r_2 = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \cong C_2 \times C_2.$$



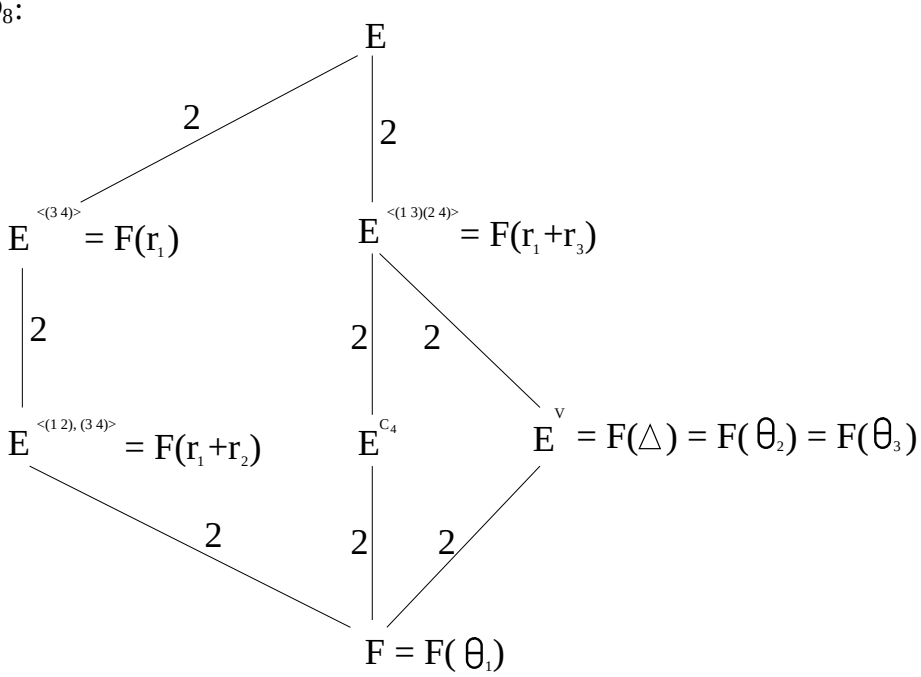
For $G = A_4$:

In this case,

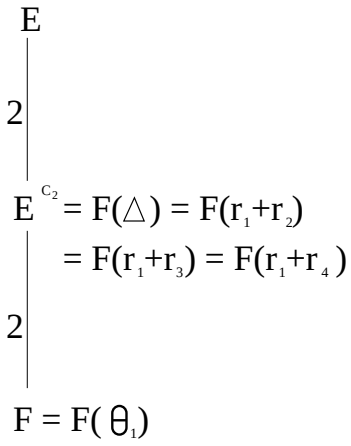
$V = G(E, F(\theta_1))$ = isotropy group of θ_1.



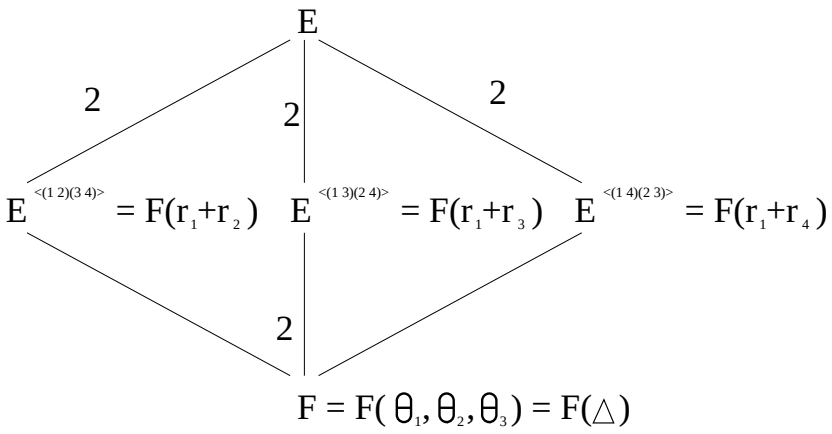
For $G = D_8$:



For $G = C_4$:



For $G = C_2 \times C_2$:



3.16 Resultants and Discriminants

Let F be a field. Let $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ belong to $F[x]$.

Let $d(x) = \gcd(f(x), g(x))$. Suppose $\deg d(x) > 0$. Write

$$f(x) = b(x)d(x),$$
$$g(x) = a(x)d(x),$$

with $\deg b(x) < n$, $\deg a(x) < m$. Then

$$a(x)f(x) = a(x)b(x)d(x) = b(x)g(x).$$

Conversely, suppose $\exists a(x), b(x)$ s.t. $\deg a(x) < m, \deg b(x) < n.$ and

$$a(x)f(x) = a(x)b(x)d(x) = b(x)g(x).$$

So $f(x) \mid b(x)g(x)$. If $\gcd(f(x), g(x)) = 1$ then $f(x) \mid b(x)$, contradicting $\deg b < \deg f$. Thus:

Proposition 3.16.1. *$f(x), g(x)$ have a common factor $\iff \exists a(x), b(x)$ s.t.*

$$a(x)f(x) = b(x)g(x),$$

with $\deg a < \deg g$ *and* $\deg b < \deg f$.

Let $a(x)f(x) = b(x)g(x)$ with

$$a(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{m-1}x^{m-1},$$
$$b(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1},$$

(coeffs. $\alpha_j, \beta_j \in F$, possibly are 0). So

$$\sum_{k=0}^{n+m-1} \left(\sum_{j=0}^{k} \alpha_{k-j} a_j \right) x^k = a(x)f(x) = b(x)g(x) = \sum_{k=0}^{n+m-1} \left(\sum_{j=0}^{k} \beta_{k-j} b_j \right) x^k.$$

That is,

$$\sum_{j=0}^{k} \alpha_{k-j} a_j - \sum_{j=0}^{k} \beta_{k-j} b_j = 0 \qquad \text{for } k = n+m-1, n+m-2, \ldots, 0.$$

Treat this as a system of $n+m$ equations in the $n+m$ variables $\{\alpha_{m-1}, \ldots, \alpha_0, \beta_{n-1}, \ldots, \beta_0\}$. Then the existence of a common factor of $f(x), g(x)$ is equivalent to the existence of a non-zero solution to this

system.
$\therefore$ Common factor exists $\iff$ determinant of this system is zero.

The determinant of the system is

$$\text{Det} = \begin{vmatrix} a_n & 0 & \cdots & 0 & -b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \ddots & \vdots & -b_{m-1} & -b_m & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ a_0 & & & a_n & & & & \\ & & & & -b_0 & & & -b_m \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & -b_0 \end{vmatrix}.$$

Multiply by $(-1)^m$ and transpose to get:

Proposition 3.16.2. *$f(x), g(x)$ have a common factor* $\iff$

$$R(f,g) := \begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & & & a_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & a_n & \cdots & \cdots & & a_0 \\ b_m & b_{m-1} & \cdots & & b_0 & & & \\ & b_m & & & & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & & b_m & \cdots & \cdots & b_0 \end{vmatrix} = 0.$$

$R(f,g)$ is called the **resultant** of f and g. Denote

$$R = \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & & & a_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & a_n & \cdots & \cdots & & a_0 \\ b_m & b_{m-1} & \cdots & & b_0 & & & \\ & b_m & & & & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & & b_m & \cdots & \cdots & b_0 \end{pmatrix},$$

so that $R(f,g) = \det R$.

$$R\begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} a_n x^{n+m-1} + a_{n-1}x^{n+m-2} + \cdots + a_0 x^{m-1} \\ a_n x^{n+m-2} + a_{n-1}x^{n+m-3} + \cdots + a_0 x^{m-2} \\ \vdots \\ a_n x^n + \cdots + a_0 \\ b_m x^{n+m-1} + \cdots + b_0 x^{n-1} \\ \vdots \\ b_m x^m + \cdots + b_0 \end{pmatrix} = \begin{pmatrix} x^{m-1}f(x) \\ x^{m-2}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ \vdots \\ g(x) \end{pmatrix}. \qquad (*)$$

Let $\tilde{R}$ be the matrix of cofactors of R. That is,

$(\tilde{R})_{ij} = \det\Big((n+m-1)\times(n+m-1)$ matrix formed by deleting row j and column i from $R\Big)$.

So $\tilde{R}R = R\tilde{R} = (\det R)I$. Apply $\tilde{R}$ to (*) gives

$$(\det R)\begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} = \tilde{R}\begin{pmatrix} x^{m-1}f(x) \\ x^{m-2}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ \vdots \\ g(x) \end{pmatrix} = \begin{pmatrix} * \\ \vdots \\ * \\ \gamma_1 x^{m-1}f(x) + \cdots + \gamma_m f(x) + \gamma_{m+1}x^{n-1}g(x) + \cdots + \gamma_{n+m}g(x) \end{pmatrix},$$

where

$$\tilde{R} = \begin{pmatrix} * & \cdots & * \\ \vdots & & \vdots \\ * & \cdots & * \\ \gamma_1 & \cdots & \gamma_{n+m} \end{pmatrix}.$$

Equating the bottom row gives

$$\det R = r(x)f(x) + s(x)g(x)$$

for some polynomials $r(x)$, $s(x)$.

Let $r_1, \ldots, r_n$ be the roots of $f(x)$ and let $t_1, \ldots, t_m$ be the roots of $g(x)$. If $r_i = t_j$ for any i and j then in an extension field, $f(x)$ and $g(x)$ have a common factor, so $\det R = 0$. For all i, j, $r_i - t_j$ divides $\det R$ in the splitting field of $f(x)g(x)$. By comparing degrees, up to a scalar multiple λ,

$$\det R = \lambda \prod_{i,j}(r_i - t_j).$$

By comparing the lead coefficient, find $\lambda = a_n^m b_m^n$. Thus:

Theorem 3.16.3. $R(f,g) = \det R = a_n^m b_m^n \prod_{i,j}(r_i - t_j)$.

Since $f(x) = a_n \prod_{i=1}^{n}(x - r_i)$ and $g(x) = b_n \prod_{j=1}^{m}(x - t_j)$, we get:

Corollary 3.16.4.

1. $R(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(r_i - t_j) = a_n^m \prod_{i=1}^{n}\left(b_m \prod_{j=1}^{m}(r_i - t_j)\right) = a_n^m \prod_{i=1}^{n} g(r_i)$, *and*
2. $R(f,g) = (-1)^{nm} b_m^n \prod_{j=1}^{m}\left(a_n \prod_{i=1}^{n}(t_j - r_i)\right) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(t_j)$.

Let $f(x)$ be monic and let $g(x) = f'(x)$.

$$f'(x) = \sum_{k=1}^{n}(x - r_1)(x - r_2)\cdots\widehat{(x - r_k)}\cdots(x - r_n).$$

So

$$f(r_i) = \prod_{\{j|j\neq i\}}(r_i - r_j).$$

Hence

$$R(f, f') = \prod_{i=1}^{n} f'(r_i) = \prod_{i}\prod_{\{j|j\neq i\}}(r_i - r_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{(i,j)|i<j}(r_i - r_j)^2 = (-1)^{\frac{n(n-1)}{2}} D,$$

where D is the discriminant. So,

$$D = (-1)^{\frac{n(n-1)}{2}} R(f, f').$$

Example 3.16.5.

$n = 2$: $f(x) = x^2 + bx + c$.

$$D = (-1)\begin{vmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2 & b \end{vmatrix} = -(b^2 + 4c - 2b^2) = b^2 - 4c.$$

$n = 3$: $f(x) = x^3 + px + q$.

$$D = (-1)\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix}$$

$$= -\begin{vmatrix} 1 & 0 & p & q \\ 0 & p & 0 & 0 \\ 3 & 0 & p & 0 \\ 0 & 3 & 0 & p \end{vmatrix} - 3\begin{vmatrix} 0 & p & q & 0 \\ 1 & 0 & p & q \\ 3 & 0 & p & 0 \\ 0 & 3 & 0 & p \end{vmatrix}$$

$$= -p\begin{vmatrix} 1 & p & q \\ 3 & p & 0 \\ 0 & 0 & p \end{vmatrix} + 3p\begin{vmatrix} 1 & p & q \\ 3 & p & 0 \\ 0 & 0 & p \end{vmatrix} - 3q\begin{vmatrix} 1 & 0 & q \\ 3 & 0 & 0 \\ 0 & 3 & p \end{vmatrix}$$

$$= 2p\begin{vmatrix} 1 & p & q \\ 3 & p & 0 \\ 0 & 0 & p \end{vmatrix} - 3q\begin{vmatrix} 1 & 0 & q \\ 3 & 0 & 0 \\ 0 & 3 & p \end{vmatrix}$$

$$= 2p^2\begin{vmatrix} 1 & p \\ 3 & p \end{vmatrix} + 9q\begin{vmatrix} 1 & q \\ 3 & p \end{vmatrix}$$

$$= 2p^2(-2p) + 9q(-3q)$$

$$= -4p^3 - 27q^2.$$

3.17 Reduction Mod p

Theorem 3.17.1. *Let $f(x) \in \mathbb{Z}[x]$ be monic with $n = \deg f$. Let E be the splitting field of $f(x)$ over $\mathbb{Q}$. Let p be a prime not dividing the discriminant d of f. (In particular, $d \neq 0$ or no such p exists.) Let $f_p(x) \in \mathbb{F}_p[x]$ be the reduction of $f(x)$ modulo p. Let E_p be the splitting field of $f_p(x)$ over $\mathbb{F}_p$. Let R and R_p be the set of roots of $f(x)$, $f_p(x)$ in E, E_p respectively. Let $D \subset E$ be the smallest subring of E containing R. Then*

1. *$\exists$ a ring homo. $\psi : D \mapsto\!\!\!\!\rightarrow E_p$.*
2. *Any such ψ gives a bijection $R \overset{1\text{-}1}{\longmapsto} R_p$.*
3. *If ψ, ψ' are two ring homos. satisfying 1 then $\exists \sigma \in G(E, \mathbb{Q})$ s.t. $\psi' = \psi\sigma$.*

Proof. 1. In E, write

$$f(x) = (x - r_1) \cdots (x - r_n)$$

with $R = \{r_1, \ldots, r_n\}$. The r_i's are distinct since $d \neq 0$. Let

$$D = \mathbb{Z}[r_1, \ldots, r_n] = \mathbb{Z}\text{-linear span in } E \text{ of elts. } r_1^{e_1} \cdots r_n^{e_n}.$$

Since $f(r_j) = 0$, r_j^n can be expressed as a $\mathbb{Z}$-linear comb. of r_j^m with $m < n$; so we may use the span of elts. of the above form with $e_j < n \; \forall j$. D is torsion-free, since $D \subset E$, and so it is a f.g. torsion free $\mathbb{Z}$-module. So

$$D = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_N,$$

for some basis $u_1, \ldots, u_N$.

Claim. $\{u_j\}$ forms a basis for E over $\mathbb{Q}$.

Proof. Any relation over $\mathbb{Q}$ among the u_j's gives, after clearing denominators, a relation over $\mathbb{Z}$. Hence $\{u_j\}$ is linearly indep. over $\mathbb{Q}$.

Let

$$S = \mathbb{Q}u_1 \oplus \cdots \oplus \mathbb{Q}u_N.$$

S is a subring of E containing $\mathbb{Q}$, and every elt. of S is algebraic over $\mathbb{Q}$. So the inverse of each elt. is a poly. in that elt. So S is a field. Since $r_j \in S \; \forall j$, $S = E$.

Proof of theorem (cont.) By the claim, $[E : \mathbb{Q}] = N$. Let

$$pD = \mathbb{Z}(pu_1) \oplus \mathbb{Z}(pu_2) \oplus \cdots \oplus \mathbb{Z}(pu_N) \subset D,$$

so $p \in \text{Ann}(D/pD)$. pD is an ideal in D and $|D/pD| = p^N$. Let M be a maximal ideal of D containing pD. Then

$$\frac{D/pD}{M/pD} \cong D/M,$$

so $|D/M|$ divides p^N, and $p \in \text{Ann}(D/M)$. Thus the field D/M has characteristic p.

$$\mathbb{Z}[r_1, \ldots, r_n] = D \quad \overset{\psi}{\longmapsto\!\!\!\!\!\rightarrow} \quad D/M.$$

So $D/M \cong (\mathbb{Z}/p)[\overline{r_1}, \ldots, \overline{r_n}]$, where $r_j := \psi r_j$.

$$\therefore \ \psi(f(x)) = (x - \overline{r_1}) \cdots (x - \overline{r_n})$$

is a factorization of $f_p(x)$ in the extension field D/M of $\mathbb{F}_p$. Hence $D/M = E_p$.

Let $\psi : D \mapsto E_p$ be a homomorphism. $\psi|_{\mathbb{Z}}$ is reduction mod p, so

$$f_p(x) = \psi(f(x)) = (x - \psi(r_1)) \cdots (x - \psi(r_n)).$$

Hence $\{\psi(r_j)\}$ are the roots of $f_p(x)$. That is, $\{\psi(r_j)\} = R_p$, so $\psi : R \overset{1\text{-}1}{\longmapsto} R_p$.

Let $\psi : D \mapsto E_p$. Let $\sigma \in G = G(E, \mathbb{Q})$. σ permutes roots, so $\sigma : D \mapsto D$. If $\sigma \neq \sigma'$ then σ, σ' are different permutations of the roots, so since ψ is a bijection on roots, $\psi\sigma \neq \psi\sigma'$.

Let

$$G = \{\sigma_1, \ldots, \sigma_N\}.$$

Then $\psi_1 = \psi\sigma_1, \ldots, \psi_N = \psi\sigma_N$ are N distinct ring homomorphisms. Suppose

$$\psi' : D \mapsto E_p$$

is a ring homo distinct from $\psi_1, \ldots, \psi_N$. Then $\{\psi_1, \ldots, \psi_N, \psi'\}$ are linearly independent in $\hom_{\mathbb{Z}}(D, E_p)$ (by Theorem 3.8.2).

However,

$$x_1\psi_1(u_j) + x_2\psi_2(u_j) + \cdots + x_N\psi_N(u_j) + x_{N+1}\psi'(u_j) = 0 \quad 1 \leq j \leq N$$

forms a system of N equations in $N+1$ variables in E_p, so it has a nontrivial solution $(a_1, \ldots, a_{N+1})$ in E_p. For an arbitrary element $y = \eta_1 u_1 + \eta_2 u_2 + \cdots + \eta_N u_N \in D$,

$$\psi_i(y) = \overline{\eta_1}\psi_i u_1 + \overline{\eta_2}\psi_i u_2 + \cdots + \overline{\eta_N}\psi_i u_N.$$

$\therefore a_1\psi_1(y) + a_2\psi_2(y) + \cdots + a_N\psi_N(y) + a_{n+1}\psi'(y) = \sum_j \sum_i \eta_j a_i \psi_i(u_j) = \sum_j \eta_j \cdot 0 = 0$. Hence,

$$a_1\psi_1 + a_2\psi_2 + \cdots + a_N\psi_N + a_{N+1}\psi' = 0$$

in $\hom_{\mathbb{Z}}(D, E_p)$, contradicting the linear independence of $\{\psi_1, \ldots, \psi_N, \psi'\}$.

So $\psi_1, \ldots, \psi_N$ is the complete list of ring homos. from D to E_p. ie. Any ring homo. $\psi' : D \mapsto E_p$ equals $\psi\sigma$ for some $\sigma \in G$.

□

Theorem 3.17.2. *Let $f(x) \in \mathbb{Z}[x]$ be monic. Let p be prime s.t. $p \nmid$ discriminant of $f(x)$. Suppose that in $\mathbb{Z}/p[x]$, $f_p(x)$ factors as*

$$f_p(x) = g_1 g_2 \cdots g_r,$$

where g_j is irreducible. Let $n_j = \deg g_j$, so $n = \deg f = n_1 + \cdots + n_r$. Then in $G = \mathrm{Gal}(f(x)) \subset S_n$, there is a permutation whose cycle decomposition (after suitably ordering the roots) is

$$(1\ 2\ \cdots\ n_1)(n_1+1\ \cdots\ n_1+n_2)(n_1+n_2+1\ \cdots\ n_1+n_2+n_3)\cdots(n_1+\cdots+n_{r-1}+1\ \cdots\ n_1+\cdots+n_r).$$

Example 3.17.3.

1. *Let $f(x) = x^3 - 2$. For $p = 5$,*

$$f_5(x) = (2+x)(4+3x+x^2)$$

$\therefore$ G contains (using some ordering of the roots) the permutation $(1)(2\ 3)$*, usually written just* $(2\ 3)$*. ie. G contains a transposition.*

For $p = 7$, $f_7(x) = x^3 + 5$, which is irreducible. So G contains (using some ordering of the roots, not necessarily the same one as before) the cycle $(1\ 2\ 3)$*. ie. G contains a* 3*-cycle.*

This identifies G as S_3 since no proper subgroup of S_3 contains both a 3*-cycle and a transposition.*

2. *Let $f(x) = x^3 - 12x + 8$. For all primes, either $f(x)$ is irreducible mod p (yielding a* 3*-cycle* $(1\ 2\ 3) \in G$*) or $f(x)$ splits linearly (corresponding to the identity in G). For no prime does it factor as an irreducible quadratic and a linear factor.*

Proof. Let $\phi : E_p \mapsto E_p$ be the Frobenius automorphism $\phi(x) = x^p$. Let $\psi : D \mapsto E_p$ be a ring homomorphism. Then so is $\phi\psi$. By the preceding theorem, $\exists \sigma \in G$ s.t. $\phi\psi = \psi\sigma$.

Restricted to $R = \{\text{roots}\}$, ψ has an inverse, so we get

$$\sigma = \psi^{-1}\phi\psi,$$

when restricted to R. ie. The action of ϕ as a permutation on R corresponds to that of ϕ on R_p under the bijection ψ. So the cycle decompositions are the same. ϕ maps one root of each g_j to another root of the same g_j (and its restriction to those roots is transitive). ie. The cycle decomposition of ϕ is as shown, and therefore so is that of σ. □

Example 3.17.4. *Let* $f(x) = x^5 - 5x + 12$. *Since* f *is irreducible, G contains a* 5*-cycle.*

$$f_3(x) = x(2 + x + x^2)(2 + 2x + x^2).$$

$\therefore$ *G contains a product of* 2*-cycles,* (1 2)(3 4) *(in some ordering).*

We can search for other primes which might give other decompositions, but we don't find any (except for complete factorizations into linear pieces, corresponding to $e \in G$*). How do we know when to stop? According to Chebotorev Density Theorem, every decomposition that appears must appear at least once for some prime* $\leq 70(\log d)^2$*, where d is the discriminant. In this case,* $70(\log d)^2 \approx 22616$*, which by the Prime Number Thm. includes approximately the first* $2256 \approx \log(22616)$ *primes. In fact, the* 2526^{th} *prime is* $22619 > 22616$*. So if we haven't found any other cycle decompositions in the first* 2525 *primes then there aren't any others. Since the only subgroups of* S_5 *containing only the* 5*-cycles, products of two* 2*-cycles, and the identity are the copies of* D_5*,* $G = D_5$ *for*

$$f(x) = x^5 - 5x + 12.$$